Guías para la implantación de un efectivo Gobierno de TI

Víctor Manuel Montaño Ardila

FOCOS DEL GOBIERNO TI

Gestión de TI

COMPONENTES DEL GOBIERNO DE TI

ebooks

CUC
CORPORACION UNIVERSITARIA DE LA COSTA
INSTITUCION DE EDUCACION SUPERIOR

Guías para la implantación de un efectivo Gobierno de TI

Guías para la implantación de un efectivo Gobierno de TI

Víctor Manuel Montaño Ardila

CUC
CORPORACION UNIVERSITARIA DE LA COSTA

2010

Guías para la implantación de un efectivo Gobierno de TI

Autor: **Víctor Manuel Montaño Ardila**

CORPORACIÓN UNIVERSITARIA
DE LA COSTA CUC
Barranquilla - Colombia - Sur América

ISBN: 978-958-8710-51-8

Primera Edición
Editorial Universitaria de la Costa EDUCOSTA
Corporación Universitaria de la Costa CUC
Calle 58 No. 55-66
Teléfono: (575) 344 4623
educosta@cuc.edu.co

Coordinación Editorial:
Perla Isabel Blanco Miranda
pblanco1@cuc.edu.co

Corrector de Estilo:
Nury Ruiz Bárcenas
nruizbarcenas@yahoo.com

Diagramación y Diseño:
Carlos Guillermo Peña Estrada
dolores-lopez@hotmail.es

Diseño y Fotografía de Portada:
Vanexa Romero
vanexares@gmail.com

Impreso por:
Yoyobiz Creativos Ltda.
yoyobizcreativos@hotmail.com

Agradecimientos

A la Ingeniera María Angélica Urán por su valioso aporte en la construcción de las Guías.

Al Ingeniero Lucio Molina Focaccio por su asesoría en la selección de referentes conceptuales.

A mis compañeros del Grupo de Investigación GICADE por su constante apoyo y motivación.

Dedicatoria

A Dios, fuente permanente de inspiración, perseverancia y fortaleza.

A mi esposa, por ser la compañera ideal y una bendición divina.

A mis hijos, por demostrarme que cuando los alumnos superan al modelo lo obligan a crecer.

A mis padres, por su confianza, apoyo y muestra de orgullo

A mis alumnos por ser fuente de deseos de superación y conocimiento.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

La disponibilidad de información de calidad para el soporte y definición de estrategias que coadyuven al fortalecimiento y consolidación de las organizaciones modernas es una de las mayores preocupaciones de los niveles estratégicos, y la tecnología informática como contenedora de este componente vital se erige como un factor crítico del éxito de las empresas.

La aplicación de tecnología contribuye a incrementar la oportunidad en la entrega de la información, pero ¿cumple realmente la información recibida con los niveles de calidad necesarios para reducir la incertidumbre?, ¿puede la organización tener tranquilidad de que la información que le está generando ventaja estratégica se encuentra adecuadamente protegida contra accesos ajenos o por pérdida de la misma?, ¿la información producida por los sistemas informáticos cumple con los requerimientos solicitados por los organismos de control? Estas son algunas de las preguntas que preocupan a la Gerencia Ejecutiva y para la obtención de respuestas tranquilizadoras asignan altos presupuestos que dejan algunas veces la sensación de que son inacabables y que nunca se recuperará lo invertido.

Por estas razones la responsabilidad para la gestión de tecnología informática (TI) ha dejado de ser sólo responsabilidad del área de tecnología, hoy la Gerencia Ejecutiva asume responsabilidades en la planeación

y en la rendición de cuentas de los resultados de TI. Por la implantación de estas modernas estructuras administrativas orientadas a proveer mayor control sobre la aplicación y resultados de TI, consolida hoy el término de Gobierno de TI.

A nivel mundial muchas organizaciones han ideado modelos orientados a facilitar la labor de la Gerencia Ejecutiva y de otros interesados en lo relativo a TI. Siendo tan extenso al ámbito de acción de TI no existe un modelo que abarque todos los aspectos relacionados, por ello la selección y aplicación de alguna de las propuestas podría dejar brechas en el modelo que facilitarían la presencia de riesgos que atentaran contra el logro de los objetivos corporativos.

COBIT provee un modelo de amplio reconocimiento a nivel mundial, pero deja muchos aspectos sin cubrir. Podríamos decir que COBIT plantea **qu**é debe hacerse para obtener un adecuado modelo de Gobierno de TI, pero quienes lo adoptan se quedan sin aterrizar ideas por cuanto desconocen **cómo** materializar lo planteado, respuesta que es provista por otras normas y/o estándares.

Existen modelos y normas que apuntan más al detalle, pero que igualmente han sido consideradas a nivel mundial como mejores prácticas. Estas propuestas al ser mapeadas con COBIT, evidencian aspectos comunes que pueden utilizarse como puntos de articulación y ser la base para la construcción de un modelo articulado de mayormente robusto que la aplicación individual de cualquiera de ellos.

Este libro pretende mostrar la construcción de unas guías para la estructuración de un modelo de Gobierno de TI basado en COBIT, marco de referencia para el Gobierno de TI, como eje central, pero fortaleciendo lo relativo a la seguridad de la información, principal recurso de las organizaciones modernas, con las propuestas formuladas por la Norma ISO 27002, que plantea un marco de referencia de objetivos de control para el efecto.

La propuesta se fortalece con las actividades planteadas por las guías de aseguramiento de COBIT, ya que éstas proveen sugerencias específicas para el cumplimiento de los objetivos de control de los procesos de TI que plantea COBIT.

Ésta será una primera propuesta, ya que el interés del autor es el de identificar otros modelos, marcos de referencia y/o normas que puedan ser articulados con COBIT y poder ofrecer a las organizaciones una herramienta articulada con sólidos fundamentos conceptuales que permitan la conformación de un modelo de Gobierno de TI muy cercano a lo ideal.

Capítulo 1

Gobierno de Tecnología Informática

GOBIERNO DE TECNOLOGÍA INFORMÁTICA

Retos de la Tecnología Informática

De acuerdo con los expertos, destacando dentro de ellos a Peter Drucker con su libro *La Sociedad Postcapitalista*, en la actual Era del Conocimiento que vive la humanidad, la información se ha convertido en el principal recurso de las organizaciones modernas. “Quien tiene la información tiene el poder” es una frase que ha hecho curso y frecuentemente es escuchada en cualquier ámbito del desempeño humano.

Con esta premisa como fundamento es imprescindible para las organizaciones modernas contar con herramientas que les permitan manejar de forma efectiva y eficiente su principal recurso o de lo contrario no podrá aprovechar las ventajas estratégicas que de él podría extraer. Así las cosas, la tecnología informática (TI) pasa a convertirse en uno de los principales factores críticos del éxito de las organizaciones y debe ser adecuadamente

administrada para lograr su óptimo apoyo al cumplimiento de los objetivos estratégicos corporativos.

Las organizaciones constantemente, y, cada vez con mayor frecuencia, deben enfrentar el reto de adaptarse con la mayor celeridad posible a las dinámicas demandas del negocio, generadas por las cambiantes condiciones de un mercado globalizado. Una respuesta tardía podría conducirla a pérdidas significativas y por qué no a la quiebra definitiva. Una buena gestión de TI provee la información necesaria para que las organizaciones puedan asumir una posición proactiva y estar un paso adelante de la competencia.

Entonces la adecuada gestión de TI es la clave para lograr dicho propósito y por ello las organizaciones modernas deben establecer un buen Gobierno de TI, entendiendo éste como ***el establecimiento de una estructura de relaciones y procesos para dirigir y controlar la empresa, con el objeto de alcanzar los objetivos corporativos y agregar valor mientras se equilibran los riesgos y el retorno sobre Tecnología Informática (TI) y sus procesos .*** El Gobierno de TI es responsabilidad de la Junta Directiva y la Gerencia Ejecutiva, quienes deben definir una dirección de TI acorde con los requerimientos de la Gerencia y establecer los controles necesarios para que se cumplan, establecer claramente quiénes son los responsables de las tareas específicas, definir niveles autorización y responsables para tomar decisiones y rendir cuentas sobre los resultados de la tareas específicas, e identificar y/o aprobar los procesos y procedimientos necesarios para administrar efectivamente TI.

Todo lo anterior teniendo en cuenta y logrando la total satisfacción de los intereses y preocupaciones de los “stakeholders” (interesados) de la organización, los cuales existen a nivel interno y externo.

Stakeholders Internos

- ✓ Junta Directiva, Gerentes ejecutivos y de Negocios
- ✓ Gerente de TI
- ✓ Gerente de Riesgo y Cumplimiento
- ✓ Auditor de TI

Stakeholders Externos

- ✓ Clientes
- ✓ Proveedores
- ✓ Auditor Externo
- ✓ Reguladores

Áreas de Enfoque del Gobierno de TI

Las actividades que posee el Gobierno de TI pueden agruparse en cinco categorías claramente definidas.

Alineamiento Estratégico

Se enfoca en asegurar que exista un total alineamiento entre el Plan Estratégico de Tecnología Informática (PETI) y el Plan Estratégico Corporativo. Mantener y validar la proposición de valor de TI y asegurando que la inversión en TI está acorde con los objetivos de la organización.

Entrega de Valor

Asegurar que la proposición de valor se cumple a través de todo el ciclo de entrega, es decir, asegurar que TI entrega los beneficios acordados, alineados con la estrategia, concentrándose en la optimización de costos y demostrando el valor intrínseco de TI.

Administración del Riesgo

Asegurar que la organización identifica los riesgos que enfrenta, que tiene claramente definido los niveles de riesgo tolerable, que ha efectuado una correcta valoración de los riesgos, que ha establecido un sistema de control ajustado a las necesidades, y que se efectúan las evaluaciones a dicho sistema con la frecuencia y profundidad requerida.

Administración de recursos

Se concentra en la óptima inversión y la adecuada administración de los recursos críticos de TI: Aplicaciones, Información, Infraestructura y personas.

Medición del desempeño

Asegurar y supervisar el cumplimiento de la estrategia de implementación, el éxito en el desarrollo de proyectos, el desempeño de los procesos y la entrega de servicio. “Lo que no se mide no se controla”, si no existe una forma de medir y evaluar las actividades de TI, no es posible gobernar TI ni asegurar su alineamiento, entrega de valor, administrar los riesgos y realizar un uso efectivo de los recursos.

Características de un Buen Marco de Trabajo para TI

El marco de trabajo o marco de referencia (framework) está constituido por los fundamentos conceptuales, métricas, herramientas, procedimientos y características que soportan la construcción de un modelo. La adopción de un adecuado marco de trabajo garantiza el éxito del resultado del modelo y éste se evidencia en la aceptación que comunidad otorgue al modelo resultante.

Un buen marco de trabajo debe cumplir poseer estas cinco características:

Brindar un fuerte enfoque en el negocio

La tecnología informática debe ser el medio y no el fin, es decir, no concentrarse en la excelencia técnica sino en el alineamiento de TI con los objetivos del negocio y la medición del desempeño de TI verificando que éste apoya el logro y la expansión de la estrategia del negocio.

Estar orientado a procesos

Con esta orientación se logra contar con vistas individuales y holísticas de los procesos, mejorar la calidad de los productos y enfocarse en el mejoramiento continuo de los procesos y no en la resolución de problemas e incidentes. Además la definición, asignación y aceptación de la propiedad de los procesos facilitará mantener el control en períodos de cambios rápidos o de crisis organizacional.

Ser de aceptación general entre las organizaciones

Haber sido probado y globalmente aceptado como una contribución de TI al éxito de la organización, estar en un proceso de mejoramiento continuo para mantenerse al ritmo de las mejores prácticas y ser el resultado de una participación de profesionales de TI de todo el mundo para garantizar pluralidad de ideas y vigencia en el tiempo.

Apoyar el cumplimiento de los requerimientos regulatorios

Permitir la atención de las demandas regulatorias ocasionadas por los escándalos financieros corporativos recientes, apoyando a la Junta Directiva en la implementación, evaluación e información del estado del control interno demostrando que los controles internos funcionan apropiadamente incluyendo los relativos a las actividades de TI. Todo lo anterior proveyendo las evidencias necesarias para mostrar el cumplimiento de los requerimientos regulatorios sobre TI que soliciten los gerentes, asesores y auditores.

Manejar un lenguaje común

Proveer un glosario de términos, claramente entendible y sin ambigüedades, sobre términos propios del marco de trabajo para evitar posibles confusiones que atentaran contra el logro de los objetivos por errores en la trasmisión o interpretación de ideas entre los equipos de proyectos. Utilizar un lenguaje común contribuye con la generación de seguridad y confianza.

Capítulo 2

El Modelo COBIT y el Gobierno de TI

EL MODELO COBIT Y EL GOBIERNO DE TI

COBIT, acrónimo de Control Objetives for Information and Related Technology (Objetivos de Control para la Información y Tecnología Relacionada), es un marco de referencia para ayudar a las organizaciones a satisfacer con éxito los desafíos de los negocios. Es un producto elaborado por el IT Governance Institute ® (ITGI) de ISACA – Servig IT Governance Professionals. La primera versión se conoció en 1994, COBIT 1.0 era un marco de referencia para realizar auditorías a la tecnología informática. En 1998 se emite la versión COBIT 2.0 con un marco de trabajo que apunta a la estructuración de un adecuado sistema de control interno para TI. En el año 2000 surge la versión COBIT 3.0 que es un marco de referencia para la administración y organización de TI, en el año 2005 el marco de trabajo de la versión COBIT 4.0 apunta a la construcción e implementación de un adecuado Gobierno de TI. Esta versión fue sometida a un proceso de mejoramiento, y en el año 2007 se emite

la versión COBIT 4.1 y se espera que a comienzos de 2011 se emita la versión COBIT 5.0.

El marco de trabajo de COBIT permite asegurar la alineación de las TI con las estrategias del negocio de manera que las TI faciliten el desarrollo del mismo y maximicen la generación de beneficios, que los recursos TI sean utilizados de forma óptima y responsable y que los riesgos derivados de la función de TI son gestionados apropiadamente.

El Marco de Trabajo de COBIT

Las principales características de COBIT son: Su enfoque en el negocio, estar orientado a procesos, es totalmente basado en procesos y es guiado por la medición permanente de los procesos realizados.

COBIT posee el marco de referencia de mayor aceptación mundial para la conformación e implementación de un adecuado Gobierno de TI, ayuda a cerrar la brecha entre los riesgos del negocio, la necesidad de control y los asuntos técnicos. Brinda mejores prácticas a través de un dominio y un marco de procesos y presenta las actividades en una estructura lógica y manejable.

COBIT constituye un apoyo no sólo para los usuarios técnicos sino también para aquellos que son responsables del uso efectivo de las TI, tales como la gerencia o la auditoría. El marco de trabajo de COBIT ayuda a estos usuarios al asegurar que sus requerimientos son apropiadamente entendidos y definidos y todos se encuentran en sintonía por utilizar un modelo comúnmente entendido.

El marco de trabajo de COBIT está basado en la premisa que TI necesita entregar información de calidad (oportuna y confiable) para la toma de decisiones y el cumplimiento de los objetivos corporativos. ***Ver Figura Nº 1.***

Adicionalmente el marco de trabajo de COBIT ayuda a obtener alineamiento de TI con el negocio, ya que se enfoca en los requerimientos de información del negocio y la organización de los recursos de TI. El objetivo fundamental es facilitar el Gobierno de TI para entregar valor desde TI al mismo tiempo que se administran los riesgos, lo cual coincide con la definición de Buen Gobierno de TI que expresamos en la sesión 1.1 (El Reto de la tecnología Informática).

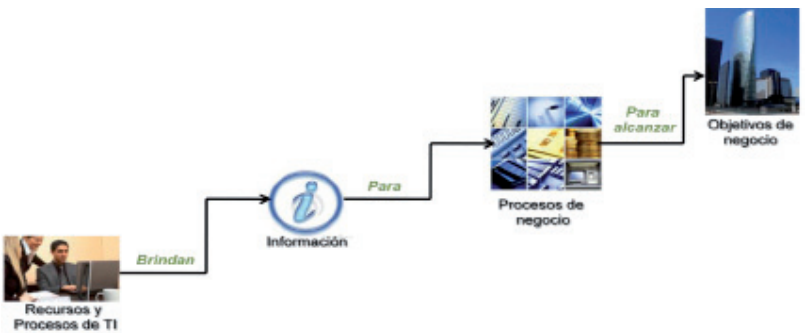


Figura Nº 1 Marco de Trabajo de COBIT

COBIT como un marco de control y Gobierno de TI se enfoca en dos áreas claves que son: Proveer la información requerida para apoyar los objetivos y requerimientos del negocio y tratar la información como el resultado de la aplicación combinada de los recursos de TI, anteriormente relacionada, y que necesitan ser administrados por los procesos.

La *Figura Nº 2* muestra los componentes de COBIT y cómo se relacionan.

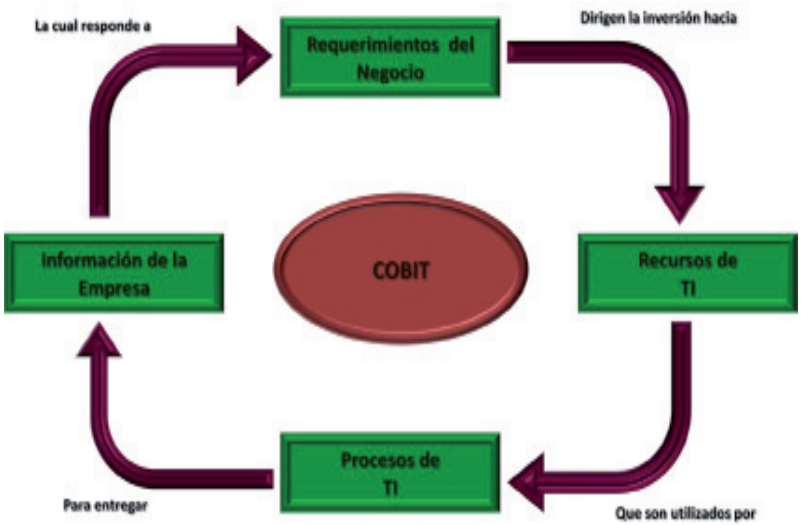


Figura Nº 2

El marco de trabajo de COBIT describe como los procesos de TI entregan la información que el negocio requiere para alcanzar sus objetivos, y para controlar dicha entrega ofrece tres componentes claves que son:

A. Criterios de Información

B. Recursos de TI

C. Procesos de TI

Estos tres componentes conforman el Cubo de COBIT que expondremos gráficamente una vez que expliquemos en detalle las características y elementos que conforman cada una de las tres caras del cubo.

A. Criterios de Información

Para satisfacer los objetivos del negocio, la información necesita cumplir con ciertos criterios de control a los que COBIT se refiere como requerimientos del negocio para la información. Son siete criterios, en algunos casos, adoptados de las propuestas de otros modelos tomados como base para la construcción del marco de referencia de COBIT tales como COSO y SAS y posteriormente clasificados en dos categorías: Fiduciarios y Seguridad.

Efectividad (Fiduciario)

Información relevante y pertinente para los procesos del negocio así como correcta, consistente, formato utilizable y entregada oportunamente.

Eficiencia (Fiduciario)

Proveer información mediante el empleo óptimo de los recursos (la mayor productividad y economía posible).

Confidencialidad (Seguridad)

Protección de la información sensible de divulgación no autorizada. La información sólo debe ser accedida por quienes la requieran para el desarrollo de sus funciones.

Integridad (Seguridad)

Información exacta y completa, así como también su validez de acuerdo con el conjunto de valores y expectativas de la empresa.

Disponibilidad (Seguridad)

La información debe estar disponible siempre en el momento en que se requiera por los procesos del negocio. Involucra la salvaguarda de los recursos y las capacidades en infraestructura y logística asociadas.

Cumplimiento (Fiduciario)

Cumplimiento de leyes, regulaciones, compromisos contractuales a los que se encuentran sujetos los procesos del negocio, ya sea en lo pertinente a la rendición de cuentas externas (informes de impuestos) como políticas internas.

Confiabilidad (Fiduciario)

Proveer información apropiada y confiable a la alta gerencia para soporte a la toma de decisiones y ejercer sus responsabilidades fiduciarias y de gobierno.

B. Recursos de TI

Los procesos de TI administran los recursos de TI para generar, entregar y almacenar la información que la organización requiere para el logro de sus objetivos. COBIT establece cuatro recursos puntuales así:

Aplicaciones

Son los procedimientos manuales y automatizados, ejecutados por los usuarios, que permiten procesar y hacer fluir la información.

Información

Es el resultado del procesamiento de los datos ingresados a los sistemas de información y que puede ser obtenido en cualquiera de las formas en que el negocio la requiera.

Infraestructura

Incluye el componente tecnológico compuesto por el hardware (equipos computacionales, redes de transmisión de datos, etc.) y el software (programas de computador, sistemas operativos, etc.) y las instalaciones donde residen estos elementos que hacen posible la labor de procesamiento de las aplicaciones.

Personas

Es el personal requerido para las funciones de planear, organizar, adquirir, implementar, brindar soporte, monitorear y evaluar los sistemas de información y los servicios que TI ofrece. Pueden ser de origen interno, tercerizado o contratado según se requiera.

C. Procesos de TI

COBIT describe el ciclo de vida de TI en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y dar soporte y Monitorear y evaluar. Cada uno de estos Dominios consta de varios Procesos y estos a su vez poseen Actividades.

Se podría decir que los Procesos son series de actividades con cortes de control naturales. Existen 34 procesos dentro de los cuatro dominios y especifican los que el negocio necesita para lograr sus objetivos. La entrega de información de cada Proceso es controlada por 34 Objetivos de Control de Alto Nivel, es decir, uno por cada proceso.

Las Actividades por su parte podemos definirlas como acciones que se requieren para obtener resultados medibles. Las Actividades tienen ciclos de vida e incluyen varias tareas medibles.

Los alcances de los cuatro dominios son:

Planear y Organizar.

Cubre las estrategias de planeación y organización, identificando la forma como las TI pueden contribuir al logro de los objetivos del negocio. La visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, para el logro de los objetivos corporativos debe implementarse una estructura organizacional y una estructura tecnológica apropiada. Este dominio y sus controles cubren los siguientes requerimientos del negocio:

- ✓ ¿Están alineadas las estrategias de las TI y del negocio?
- ✓ ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ✓ ¿Entienden todas las personas dentro de la organización los objetivos de las TI?

- ✓ ¿Se entienden y administran los riesgos de las TI?
- ✓ ¿Es apropiada la calidad de los sistemas de las TI para las necesidades del negocio?

Adquirir E Implementar.

Las soluciones a los requerimientos de TI necesitan ser identificadas, desarrolladas o adquiridas y luego ser implementadas e integradas en los procesos del negocio. Adicionalmente, deben controlarse los cambios y/o mantenimientos de los sistemas existentes que obedecen a satisfacer requerimientos de nuevas operativas del negocio. Este dominio contesta a las siguientes cuestiones:

- ✓ ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ✓ ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?
- ✓ ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ✓ ¿Los cambios afectarán las operaciones actuales del negocio?

Entregar y Dar Soporte.

Se preocupa por la entrega de los servicios requeridos, la prestación de los servicios de TI, la administración de la seguridad y de la continuidad en el funcionamiento de TI, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Este dominio trata de garantizar:

- ✓ ¿Se están entregando los servicios de las TI de acuerdo con las prioridades del negocio?
- ✓ ¿Están optimizados los costos de las TI?
- ✓ ¿Es capaz la fuerza de trabajo de utilizar los sistemas de las TI de manera productiva y segura?
- ✓ ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

Monitorear y Evaluar.

Este dominio se concentra en la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del Gobierno. Contesta a las siguientes preguntas:

- ✓ ¿Se mide el desempeño de las TI para detectar los problemas antes de que sea demasiado tarde?
- ✓ ¿La Alta Dirección garantiza que los controles internos son efectivos y eficientes?
- ✓ ¿Puede vincularse el desempeño de lo que las TI ha realizado con las metas del negocio?
- ✓ ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de Gobierno a los objetivos de la función de servicios de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT. ***La Figura Nº 3*** muestra el Cubo COBIT, que permite evidenciar la articulación expuesta.

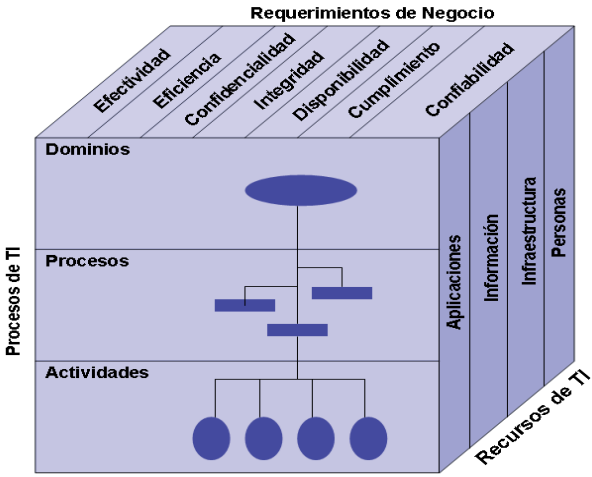


Figura Nº 3 - Cubo COBIT

Áreas de enfoque de COBIT para el Gobierno de TI

Las áreas Focales del Gobierno de TI, definen los aspectos en los que la Gerencia Ejecutiva requiere concentrar su atención para establecer un exitoso Gobierno de TI en la Organización.

Alineación estratégica

Se enfoca en garantizar el vínculo o alineamiento entre los planes del negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de valor

Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI

genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

Administración de riesgos

Requiere obtener conciencia de los riesgos por parte de la Alta Gerencia de la organización, un claro entendimiento del apetito de riesgo que tiene la empresa (riesgo tolerable), comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Administración de recursos

Se concentra en la óptima inversión en TI, así como la administración adecuada de los recursos críticos de TI: Aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Medición del desempeño

Monitorea la estrategia de implementación del Gobierno de TI, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de herramientas administrativas como el balanced scorecards, que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

Figura Nº 4 –Áreas Focales del Gobierno de TI de COBIT

Conclusiones sobre COBIT

De lo expuesto a lo largo del presente capítulo, podemos establecer conclusiones que nos conducen a que COBIT constituye un marco de trabajo ideal para la construcción e implementación de Gobierno de TI, y éstas son algunas razones:

a. Tiene las mejores prácticas aceptadas internacionalmente.
b. Es orientado a la administración.
c. Es soportado por herramientas y entrenamiento.
d. Está disponible libremente como estándar abierto.

e. Permite compartir y extraer el conocimiento de voluntarios expertos.

f. Evoluciona continuamente.

g. Es mantenido por una organización no lucrativa de gran reputación.

h. Puede mapearse 100% con el Modelo COSO.

i. Puede mapearse fuertemente con los principales estándares temáticamente. relacionados.

j. Es un marco de referencia. Flexible para su implantación.

También ofrece las siguientes ventajas:

a. COBIT puede alinearse con otros estándares y mejores prácticas y podría efectuarse una implantación conjunta.

b. El marco de trabajo de COBIT y las mejores prácticas que lo apoyan brinda un ambiente de TI flexible y bien administrado en una organización.

c. COBIT brinda un ambiente de control que responde a las necesidades del negocio y le sirve a las funciones gerenciales y de auditoría en lo relativo a sus responsabilidades de control.

d. COBIT ofrece herramientas para contribuir a la administración de las actividades de TI

Capítulo 3

Sistema de Gestión de Seguridad de la Información Norma ISO 27001

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Ya hemos expresado en el primer capítulo que la información es considerada como el principal recurso de las organizaciones y más aun cuando es un factor crucial para la generación de ventajas competitivas. Es preocupación de la alta gerencia establecer estructuras y acciones que permitan salvaguardar adecuadamente este recurso, ya que los datos y los medios de procesamiento, activos altamente vulnerables, se encuentran expuestos a amenazas que atentan contra su seguridad y por tanto afectan su disponibilidad, su integridad y su confidencialidad.

- **Disponibilidad:** La información debe estar disponible siempre en el momento en que se requiera por los procesos del negocio.

- **Integridad:** Información exacta y completa, así como también su validez de acuerdo con el conjunto de valores y expectativas de la empresa.
- **Confidencialidad:** Protección de la información sensible de divulgación no autorizada. La información sólo debe ser accedida por quienes la requieran para el desarrollo de sus funciones.

Como puede observarse, estos tres intereses a los que apunta un SGSI son plenamente coherentes con los criterios de información que se definieron para el marco de trabajo del modelo COBIT en el Capítulo 2, Sesión 2.1, Aparte A. Estos aspectos constituirán los puntos principales sobre los que se establecerá la articulación entre un modelo de Gobierno de TI, como COBIT y un Sistema de Gestión de Seguridad de la Información SGSI que ya debe intuir es a lo que apunta la Norma ISO 27000.

Siendo la información uno de sus activos más importantes para las organizaciones, la materialización de una amenaza podría comprometer seriamente la continuidad del negocio. Esta situación ha motivado a que las organizaciones reordenen sus estructuras y abran campo a nuevas disciplinas y habilidades gerenciales para responder de forma efectiva y eficiente a estos riesgos y minimizar su probabilidad de ocurrencia o reducir su impacto.

Nace entonces un decidido interés por gestionar adecuadamente la seguridad de la información y reconocidas entidades y agremiaciones de profesionales mundialmente reconocidas emiten normas

internacionales y se definen políticas locales que apuntan proveer integridad, confidencialidad y disponibilidad en la información. Las organizaciones modernas dentro de su interés por satisfacer los requerimientos informáticos de y la seguridad en la inversión de sus stakeholders deben establecer políticas encaminadas a gestionar el riesgo sobre la información y los sistemas de información que las procesan.

Para qué sirve un SGSI

El cumplimiento de las leyes y regulaciones, la exigente, constante y oportuna adaptación a las condiciones variables del entorno y la protección apropiada de los objetivos corporativos para maximizar los beneficios o el aprovechamiento de nuevas oportunidades de negocio, son algunos de aspectos fundamentales en los que un SGSI constituye una herramienta de gran utilidad e importante ayuda para la gestión de las organizaciones.

Los niveles de seguridad logrados con la aplicación de medios técnicos son limitados e insuficientes. La gestión efectiva de la seguridad de la información requiere de la participación activa de todo el recurso humano de la organización, con el liderazgo de la Gerencia Ejecutiva y considerando la participación de clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad de la información debe contemplar procedimientos claros y coherentes y la definición e implementación de controles para la seguridad basados en una efectiva evaluación de riesgos y una medición de la eficacia de los mismos. ***Ver Figura Nº 5***

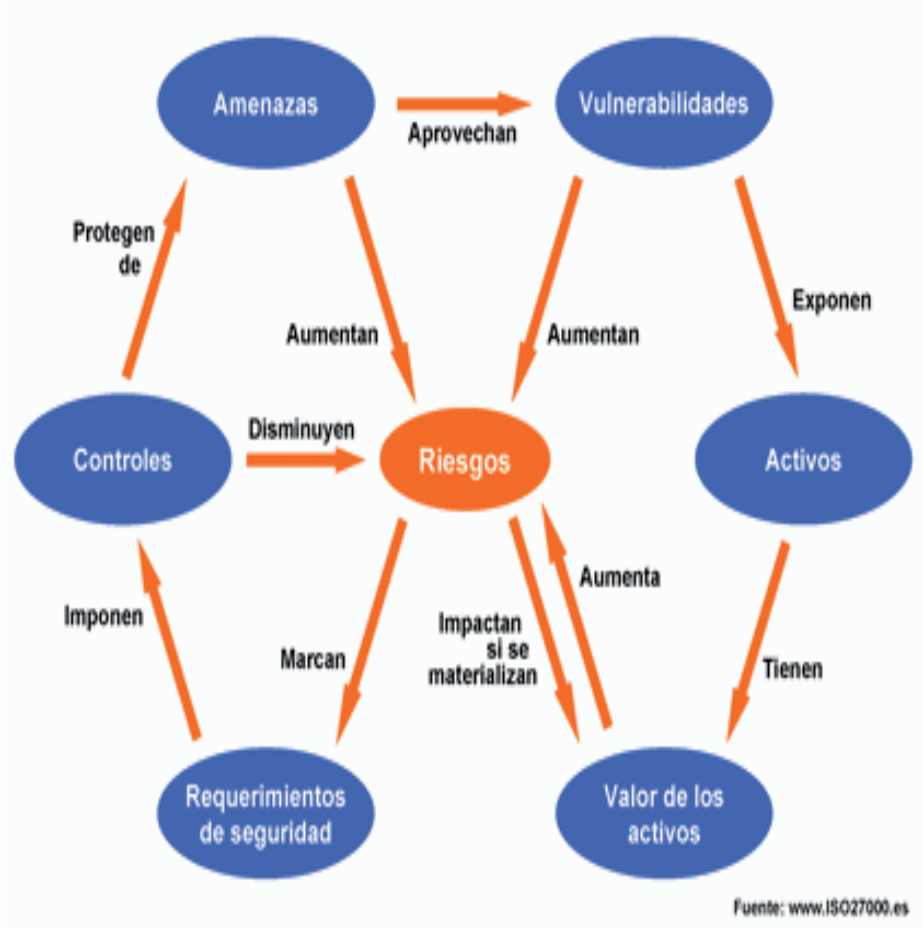


Figura Nº 5 – Componentes de un Modelo de Administración del Riesgo

El SGSI brinda las bases para el establecimiento de políticas y procedimientos relacionadas con los objetivos de negocio de la organización con el objeto de mantener un nivel de exposición al riesgo siempre menor al nivel que la organización estableció asumir.

Con la implementación de SGSI, la organización establece las amenazas y valora los riesgos a los que enfrenta su información y decide asumirlos, minimizarlos, transferirlos y/o controlarlos mediante procedimientos sistemáticamente definidos, documentados y divulgados que se revisan y mejoran constantemente[1].

Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (Norma ISO 27001)

El diseño e implementación de un SGSI dependerá de los objetivos estratégicos y de las necesidades del negocio. La decisión de iniciar el proyecto debe recibir total e irrestricto apoyo por parte de la Gerencia Ejecutiva de la organización y en gran medida el éxito del proyecto dependerá del grado de apoyo que reciba de ésta, es decir, para este tipo de proyectos el apoyo de los niveles estratégicos el requisito indispensable.

La estructura y alcance de SGSI varía con el tipo de organización y el sector económico en el que se encuentre, no obstante para su implementación y mantenimiento, sin importar el tipo de negocio u organización, debe seguirse un ciclo de mejora continua y en ese orden de ideas el ciclo PHVA (Planear, Hacer, Verificar, Actuar) ó PDCA (Plan, Do, Check, Act) ó ciclo Deming es la más recomendable alternativa. ***Ver Figura Nº 6.***

1 ICONTEC. Manual Norma ISO 27001: Sistema de Gestión de Seguridad de la Información.

Figura Nº 6 – Modelo de Gestión del Riesgo (Ciclo PDCA)

PLAN (Planear). (Establecer el SGSI)

A. Definir el alcance del SGSI tomando como argumentos el negocio, la organización, su localización, activos y tecnologías. Se incluyen detalles y justificación de cualquier aspecto o componente que se excluya.

B. Definir una política de seguridad que:

- ✓ Considera la organización en su generalidad y entorno y que establezca claramente los objetivos de seguridad de su información.
- ✓ Considere cumplimiento efectivo de requerimientos legales o contractuales relativos a la seguridad de la información.

- ✓ Se encuentre totalmente alineado con el contexto estratégico del sistema de control interno de la organización.

- ✓ Establezca los criterios y métricas con los que se evaluarán los riesgos.

- ✓ Tenga la aprobación de la dirección.

C. Definir una metodología para la evaluación del riesgo acorde con el SGSI y los requerimientos del negocio, además de establecer los criterios para aceptación del riesgo y especificar los niveles de riesgo aceptable.

D. Identificar los riesgos:

- ✓ Identificar los activos de información que se incluirán dentro del alcance del SGSI y a los responsables directos de ellos.

- ✓ Identificar las amenazas en de cada uno de dichos activos.

- ✓ Identificar las vulnerabilidades que puedan facilitar la materialización las amenazas identificadas.

- ✓ Identificar el impacto relacionado con la confidencialidad, integridad y disponibilidad de los activos.

E. Analizar y evaluar los riesgos:

- ✓ Evaluar el impacto en el negocio ocasionado por una falla en la seguridad de la información y que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

- ✓ Establecer la probabilidad de ocurrencia de una falla en la seguridad de la información relacionada con las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.
- ✓ Estimar los niveles de riesgo.
- ✓ Determinar, según los criterios de aceptación de riesgo previamente establecidos, si un riesgo es aceptable o necesita ser tratado.

F. Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- ✓ Aplicar controles coherentes con las amenazas.
- ✓ Aceptar el riesgo, siempre y cuando cumpla con las políticas y criterios establecidos para la aceptación de los riesgos.
- ✓ Establecer qué riesgos se evitarán.
- ✓ Establecer qué riesgos se transferirán a terceros.

G. Seleccionar los objetivos de control y los controles expuestos en el **Anexo A de la Norma ISO 27001** que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

H. Aprobar por parte de la dirección los riesgos residuales y la implementación y uso del SGSI.

I. Definir una declaración de aplicabilidad que incluya:

- ✓ Los objetivos de control y controles seleccionados y los motivos para su elección.

- ✓ Los objetivos de control y controles que actualmente se encuentran implantados.
- ✓ Los objetivos de control y controles del **Anexo A de la Norma ISO 27001** excluidos y los motivos para su exclusión. Esta actividad podría permitir la detección involuntaria de algún o algunos objetivos de control.

DO (Hacer). Implementar y utilizar el SGSI

A. Definir un plan de tratamiento de riesgos que establezca acciones, recursos, responsabilidades y prioridades inherentes a la gestión de los riesgos de seguridad de la información.

B. Implementar el plan de tratamiento de riesgos, orientado al logro de los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

C. Implementar los controles anteriormente seleccionados que permitan lograr los objetivos de control identificados.

D. Definir un sistema de métricas para la eficacia de los controles y cuyos resultados sean reproducibles y comparables con un patrón.

E. Procurar programas de formación, socialización y compromiso del personal en relación con la seguridad de la información.

F. Gestionar las operaciones del SGSI.

G. Gestionar los recursos necesarios asignados al SGSI.

H. Implantar procedimientos y controles que faciliten la rápida detección y respuesta a los incidentes de seguridad.

Check (Verificar). Monitorizar y revisar el SGSI

La organización deberá:

A. Ejecutar procedimientos de seguimiento y revisión para:

- ✓ Detectar oportunamente errores en los resultados del procesamiento de la información.
- ✓ Identificar vulnerabilidades e incidentes de seguridad.
- ✓ Ayudar a la dirección a verificar el cumplimiento, por parte de personas y dispositivos, de las actividades establecidas para garantizar la seguridad de la información.
- ✓ Detectar y prevenir oportunamente eventos e incidentes de seguridad mediante la aplicación de indicadores.
- ✓ Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

B. Revisar regularmente la efectividad del SGSI, verificando el cumplimiento de la política y objetivos establecidos por el SGSI, tomando como base los resultados de auditorías de seguridad, incidentes, resultados de mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

C. Medir la efectividad de los controles establecidos para verificar si cumplen los requisitos de seguridad.

D. Revisar periódicamente las evaluaciones de riesgo, los riesgos definidos como residuales y sus niveles aceptables, esto teniendo en cuenta posibles cambios producidos en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior (requerimientos legales, obligaciones contractuales, etc.).

E. Realizar, periódicamente y de manera planificada, auditorías internas del SGSI.

F. Revisar periódicamente el SGSI, por parte de la dirección, para garantizar que el alcance establecido continúa siendo válido y que se evidencian mejoras en el proceso del SGSI.

G. Actualizar los planes de seguridad con base en las conclusiones y hallazgos encontrados durante las actividades de monitorización y revisión.

H. Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act (Actuar). Mantener y mejorar el SGSI

La organización deberá regularmente:

A. Implantar en el SGSI las mejoras identificadas producto de las evaluaciones.

B. Realizar las acciones preventivas y correctivas resultantes de las lecciones aprendidas de las experiencias propias y de otras organizaciones.

C. Comunicar las acciones correctivas y las mejoras introducidas a todos los interesados utilizando un nivel de detalle y un lenguaje adecuado, y acordar, si es pertinente, la forma de proceder.

D. Asegurar que las mejoras introducidas apuntan a lograr los objetivos previstos.

Norma ISO 27002

Los estándares pertenecientes a la familia de la Norma ISO 27000 apuntan a proveer lineamientos efectivos para la Gestión de la Seguridad de la Información en las organizaciones. Como hemos expuesto en el subcapítulo anterior, la Norma ISO 27001 contiene la estructura y requerimientos para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI), mientras que la Norma ISO 27002 establece y describe los objetivos de control y controles recomendables a tener en cuenta para la construcción de un adecuado SGSI, es por esto que se considera como uno de los anexos de la ISO 27001.

El estándar internacional ISO 27002 fue publicado por la ISO *(International Organization for Standarization)* y IEC (*International Electrotechnical Commission)*, quienes configuraron un comité mixto para el efecto. Los fundamentos conceptuales históricos para el estándar fue la BS 7799-1, que a su vez tuvo como fundamento lo expuesto por Norma ISO/IEC 17799:2005 Tecnología de la Información. El Código de Prácticas para la Gestión de Seguridad de la

Información BS 7799-1:1999, fue desarrollado por la British Standards Institution (BSI) y publicado en dos partes:

I. BS 7799 Parte 1: Tecnologías de la Información – Código de Prácticas para la Gestión de Seguridad de la Información.

II. BS 7799 Parte 2: Sistemas de Gestión de Seguridad de la Información – Especificaciones con guías para su uso.

La primera edición de la Norma se publicó en el año 2000 y posteriormente actualizada en junio de 2005. Se ha clasificado como una de las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información.

El objetivo del estándar ISO/IEC 27002:2005 es brindar información fundamental para los responsables de la implementación de seguridad de la información de una organización. Los excelentes resultados obtenidos y las facilidades que brinda su implantación la ha hecho considerar como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales[2].

Consta de 133 controles de seguridad organizados en 39 categorías bajo 11 dominios y define estrategias para la implementación de cada uno de dichos controles. La Norma resalta la importancia de la gestión del riesgo, pero hace claridad en que no necesario aplicar todas sus propuestas, sino sólo las que se consideren pertinentes.

2 ICONTEC. Norma ISO 27002: Código de Prácticas para la Gestión de Seguridad de la Información

Ver Tabla Nº 1.

ISO/IEC 27002:2005. DOMINIOS, OBJETIVOS DE

5. POLÍTICA DE SEGURIDAD.
- 5.1 Política de seguridad de la información.
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
  - 6.1.4 Proceso de autorización de recursos para el procesado de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- 6.2 Terceros.
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- 7.1 Responsabilidad sobre los activos.
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- 7.2 Clasificación de la información.
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 8.1 Antes del empleo.
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- 8.2 Durante el empleo.
  - 8.2.1 Responsabilidades de la dirección.
  - 8.2.2 Concienciación, formación y capacitación en seguridad de la información.
  - 8.2.3 Proceso disciplinario.
- 8.3 Cese del empleo o cambio de puesto de trabajo.
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los de derechos de acceso.

9. SEGURIDAD FÍSICA Y AMBIENTAL.
- 9.1 Áreas seguras.
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso pú[illegible]
- 9.2 Seguridad de los equipos.
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- 10.1 Responsabilidades y procedimientos de operación.
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.
- 10.2.1 Provisión de servicios.
- 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
- 10.2.3 Gestión de cambios en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.
- 10.3.1 Gestión de capacidades.
- 10.3.2 Aceptación del sistema.

10.4 Protección contra código malicioso y descargable.
- 10.4.1 Controles contra el código malicioso.
- 10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.
- 10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.
- 10.6.1 Controles de red.
- 10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.
- 10.7.1 Gestión de soportes extraíbles.
- 10.7.2 Retirada de soportes.
- 10.7.3 Procedimientos de manipulación de la información.
- 10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.
- 10.8.1 Políticas y procedimientos de intercambio de información.
- 10.8.2 Acuerdos de intercambio.
- 10.8.3 Soportes físicos en tránsito.
- 10.8.4 Mensajería electrónica.
- 10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.
- 10.9.1 Comercio electrónico.
- 10.9.2 Transacciones en línea.
- 10.9.3 Información puesta a disposición pública.

10.10 Supervisión.
- 10.10.1 Registro de auditorías.
- 10.10.2 Supervisión del uso del sistema.
- 10.10.3 Protección de la información de los registros.
- 10.10.4 Registros de administración y operación.
- 10.10.5 Registro de fallos.
- 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.
- 11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.
- 11.2.1 Registro de usuario.
- 11.2.2 Gestión de privilegios.
- 11.2.3 Gestión de contraseñas de usuario.
- 11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.
- 11.3.1 Uso de contraseña.
- 11.3.2 Equipo de usuario desatendido.
- 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.
- 11.4.1 Política de uso de los servicios en red.
- 11.4.2 Autenticación de usuario para conexiones externas.
- 11.4.3 Identificación de equipos en las redes.
- 11.4.4 Diagnóstico remoto y protección de los puertos de configuración.
- 11.4.5 Segregación de las redes.
- 11.4.6 Control de la conexión a la red.
- 11.4.7 Control de encaminamiento de red.

11.5 Control de acceso al sistema operativo.
- 11.5.1 Procedimientos seguros de inicio de sesión.
- 11.5.2 Identificación y autenticación de usuario.
- 11.5.3 Sistema de gestión de contraseñas.
- 11.5.4 Uso de los recursos del sistema.
- 11.5.5 Desconexión automática de sesión.
- 11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.
- 11.6.1 Restricción del acceso a la información.
- 11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.
- 11.7.1 Ordenadores portátiles y comunicaciones móviles.
- 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.
- 12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.
- 12.2.1 Validación de los datos de entrada.
- 12.2.2 Control del procesamiento interno.
- 12.2.3 Integridad de los mensajes.
- 12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.
- 12.3.1 Política de uso de los controles criptográficos.
- 12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.
- 12.4.1 Control del software en explotación.
- 12.4.2 Protección de los datos de prueba del sistema.
- 12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.
- 12.5.1 Procedimientos de control de cambios.
- 12.5.2 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo.
- 12.5.3 Restricciones a los cambios en los paquetes de software.
- 12.5.4 Fugas de información.
- 12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

13.1 Notificación de eventos y puntos débiles de la segur. de la información.
- 13.1.1 Notificación de los eventos de seguridad de la información.
- 13.1.2 Notificación de puntos débiles de la seguridad.

13.2 Gestión de incidentes de seguridad de la información y mejoras.
- 13.2.1 Responsabilidades y procedimientos.
- 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
- 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
- 14.1.2 Continuidad del negocio y evaluación de riesgos.
- 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
- 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
- 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.
- 15.1.1 Identificación de la legislación aplicable.
- 15.1.2 Derechos de propiedad intelectual (DPI).
- 15.1.3 Protección de los documentos de la organización.
- 15.1.4 Protección de datos y privacidad de la información personal.
- 15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información.
- 15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de segur. y cumplimiento técnico.
- 15.2.1 Cumplimiento de las políticas y normas de seguridad.
- 15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones de las auditorías de los sistemas de información.
- 15.3.1 Controles de auditoría de los sistemas de información.
- 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Tabla Nº 1. Dominios, Objetivos de Control y Controles

La Norma ISO/IEC 27002:2005 establece principios rectores que constituyen su base para la implementación de la seguridad de la información y estos tienen su fundamentación en los requerimientos legales o en las mejores prácticas generalmente aceptadas.

Los principios establecidos por requisitos legales son:

a. La protección y la no divulgación de datos personales.
b. Protección de la información interna.
c. Protección de los derechos de propiedad intelectual.

Los fundamentos de las mejores prácticas aplicadas por la Norma ISO/IEC 27002:2005 incluyen:

a. La política de seguridad de la información.
b. Asignación de la responsabilidad de seguridad de la información.
c. Escalamiento de problemas.
d. Gestión de la continuidad del negocio.

Existen aspectos crucialmente importantes al momento de implementar un sistema de gestión de seguridad de la información y su consideración constituye un factor crítico de éxito para el proceso:

a. La política de seguridad, sus objetivos y actividades deberían reflejar los objetivos de negocio.
b. La implementación debería considerar los aspectos culturales de la organización.

c. Se requiere un abierto apoyo y el compromiso de la alta dirección.

d. Se requiere un conocimiento exhaustivo de los requisitos de seguridad, evaluación del riesgo y gestión del riesgo.

e. El marketing efectivo de la seguridad debe dirigirse a todo el personal, incluidos los miembros de la dirección.

f. La política de seguridad y las medidas de seguridad deben ser comunicadas a terceros contratados.

g. Los usuarios deben ser capacitados en forma adecuada.

h. Se debería disponer de un sistema integral y balanceado para la medición del desempeño, que apoye la mejora continua de suministro de información.

Capítulo 4

Guías de Aseguramiento de COBIT

GUÍAS DE ASEGURAMIENTO DE COBIT

El objetivo de las Guías de Aseguramiento es proporcionar orientación sobre la forma de aplicar COBIT para apoyar una variedad de actividades de aseguramiento de TI. Si la organización ya está utilizando COBIT como marco para el Gobierno de TI, se facilitará la aplicación de las Guías de Aseguramiento desde la planificación de TI, ya que el negocio, los profesionales responsables de la seguridad de TI están alineados en torno a un marco común y objetivos comunes.

Las Guías de Aseguramiento están diseñadas para permitir el desarrollo eficiente y eficaz de las iniciativas de seguridad de TI, proporcionando orientación sobre la planificación, alcance y ejecución de estudios de control utilizando una hoja de ruta basada en la garantía que brinda utilizar los enfoques de una buena práctica. También se brinda orientación sobre cómo los recursos de COBIT pueden ser utilizados durante estas etapas con el apoyo de pruebas detalladas fundamentadas

en los procesos de COBIT y los objetivos de control. La orientación y las pruebas sugeridas, igual que los recursos de COBIT, no tienen la intención de ser obligatoriamente aplicados, sino que deben ser moldeadas para adaptarse a los requerimientos específicos.

La Guía de Aseguramiento ofrece recomendaciones para los diferentes niveles. En el nivel de proceso brinda asesoramiento en procesos específicos y proporciona formas de comprobar si los objetivos de control se están logrando y la forma de documentar las debilidades de control. En el plano de los objetivos de control, plantea métricas para evaluar lo adecuado del diseño del control, esto para cada objetivo de control tomando como base los resultados históricos de su aplicación.
Se proponen recomendaciones generales para todos los niveles y guías genéricas para todos los procesos y o objetivos de control aunque puede optarse por tomar las recomendaciones específicas que para cada uno de estos componentes se plantean[3].

Para las etapas de prueba de la fase de ejecución esta guía ofrece orientaciones genéricas, así como una orientación específica y más detallada para apoyar a los profesionales de TI. Asesoramiento genérico significa que se puede aplicar a cualquiera de los objetivos de control, de procesos, o las prácticas de control dependiendo del tipo de orientación. Una visión general del marco de referencia del aseguramiento de TI en que se basa este proceso se muestra en la ***Figura Nº 7***.

3 IT GOVERNANCE INSTITUTE. IT Assurance Guide. Using COBIT.

Componentes de la Guía de Aseguramento de TI

El contenido detallado de la guía aseguramiento se presenta en los 34 procesos de COBIT y contiene los siguientes componentes:

Objetivos de Control

Cada vez más, las organizaciones están reconociendo que ejercer un adecuado control de TI es un factor crítico para asegurar que las TI proporcionan valor a la organización, los riesgos se gestionan, los requisitos reglamentarios se cumplen, y las inversiones en TI ofrecer un rendimiento razonable.

Los Objetivos de Control son declaraciones del resultado deseado o el fin perseguido por la aplicación particular de las prácticas de control sobre los procesos de TI y por ello a menudo se relacionan directamente como actividades específicas dentro de los procesos. Los Objetivos de Control de alto nivel de COBIT son requisitos básicos a ser considerado para el control efectivo de cada proceso. Están escritos como acciones cortas orientadas a las prácticas de gestión; siempre que sea posible siguen la secuencia lógica de un ciclo de vida.

La Administración de la Empresa debe seleccionar los objetivos de control que guardan relación con la organización. Los miembros de la dirección deben:

- ✓ Seleccionar los objetivos de control aplicables.
- ✓ Determinar la inversión necesaria para implementar prácticas de gestión necesarias para alcanzar

los objetivos de control con el nivel de riesgo establecido.

- ✓ Decidir las prácticas de control a poner en práctica.
- ✓ Elegir la forma de aplicar cada una de las prácticas de control.

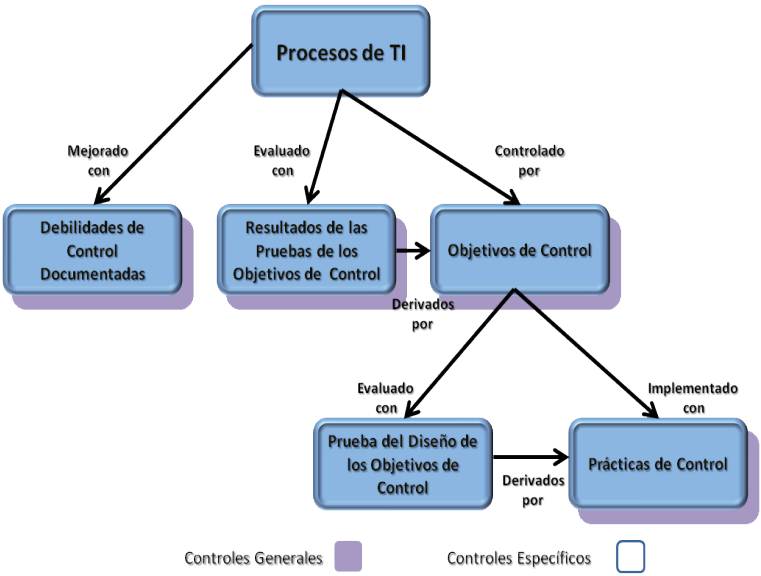


Figura Nº 7 – Vista General del apoyo provisto para el Aseguramiento de TI

RELACIÓN DE LAS GUÍAS DE ASEGURAMIENTO CON LAS PRÁCTICAS DE CONTROL

Las Guías de Aseguramiento de TI forman parte de la familia de productos que COBIT ofrece para apoyar la implantación del modelo de Gobierno de TI. Los pasos de la prueba de aseguramiento son tomados de las Prácticas de Control de COBIT.

Las Prácticas de Control de COBIT amplían las capacidades del marco COBIT y proporciona un nivel adicional de detalle. Los Procesos de TI de COBIT, los requisitos del negocio y los objetivos de control definen los requerimientos para aplicar una eficaz estructura de control.

Las Prácticas de Control de COBIT proporcionan orientación más detallada a nivel de objetivo de control sobre cómo lograr el cumplimiento de cada objetivo. Las Prácticas de Control poseen los siguientes elementos para cada uno de los objetivos de control COBIT:

- ✓ Valor y los conductores de riesgo, proporcionando una guía de ¿Por qué hacerlo?

- ✓ Las prácticas de control que deben considerarse al evaluar los procesos de TI y la implantación de mejoras.

Para cada uno de los objetivos de control se define una lista de prácticas específicas de control. Además, se definen tres prácticas de control generales que son aplicables a todos los objetivos de control. El conjunto completo de prácticas de control generales y específicas permiten un enfoque al control que consiste en prácticas que son necesarias para lograr los objetivos de control y proporcionan orientación general de del objetivo de control de alto nivel con amplio detalle para evaluar la madurez de los procesos y considerando las posibles mejoras y aplicación de los controles[4].

4 IT GOVERNANCE INSTITUTE. IT Assurance Guide. Using COBIT.

Las prácticas de control permiten asegurar que las soluciones propuestas tienen mayor probabilidad de ser completamente implementadas con éxito y proporcionar orientación sobre qué controles son necesarios y cuáles son las buenas prácticas para alcanzar los objetivos de control específicos.

Las prácticas de control están diseñadas para soportar dos intereses:

- ✓ Los implementadores de TI (por ejemplo, la gestión, los proveedores de servicios, los usuarios finales, los profesionales de control).
- ✓ Profesionales de Aseguramiento (por ejemplo, profesionales de la seguridad, interna y externa).

Para propósitos de control, todas las prácticas de control se utilizan para desarrollar los pasos detallados de aseguramiento. Los pasos son pruebas de control diseñadas por un profesional de aseguramiento interno o externo para proporcionar confiabilidad de la primera etapa de la elaboración de un programa de aseguramiento.

Capítulo 5

GUÍAS ARTICULADAS COBIT 4.1, ISO 27002

GUÍAS ARTICULADAS COBIT 4.1, ISO 27002

Las guías que proponemos a continuación surgen de una articulación entre los objetivos de control expuestos por el Marco de Referencia de COBIT con los objetivos de control de la Norma ISO 27002 en los aspectos relativos a proveer seguridad de la información relacionada la Tecnología Informática.

En el capítulo 2 mencionamos que de los siete Requerimientos de Información: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Confiabilidad y Cumplimiento, tres de ellos era comunes con los objetivos propuestos por la Norma ISO 27000 (Confidencialidad, Integridad, Disponibilidad) y son precisamente estos aspectos los que permiten una fácil articulación con criterios de los dos marcos de trabajo. A continuación expondremos por cada Dominio de COBIT y destacaremos de ellos los Procesos relacionados con la seguridad de la información utilizando un color más tenue.

Más adelante en los cuatro Apéndices, se encontrará por cada Actividad de cada Proceso perteneciente a cada Dominio, la articulación entre los dos marcos de referencia y el soporte de las acciones a ejecutar propuestas por las Guías de Aseguramiento de COBIT.

PLANEAR Y ORGANIZAR

PO1 Definir un Plan Estratégico de TI

PO2 Definir la Arquitectura de la Información

PO3 Determinar la Dirección Tecnológica

PO4 Definir los Procesos, Organización y Relaciones de TI

PO5 Administrar la Inversión en TI

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

PO7 Administrar Recursos Humanos de TI

PO8 Administrar la Calidad

PO9 Evaluar y Administrar los Riesgos de TI

PO10 Administrar Proyectos

ADQUIRIR E IMPLEMENTAR

AI1 Identificar soluciones automatizadas

AI2 Adquirir y mantener software aplicativo

AI3 Adquirir y mantener infraestructura tecnológica

AI4 Facilitar la operación y el uso

AI5 **Adquirir recursos de TI**

AI6 **Administrar cambios**

AI7 **Instalar y acreditar soluciones y cambios**

ENTREGAR Y DAR SOPORTE

DS1 **Definir y administrar los niveles de servicio**

DS2 **Administrar los servicios de terceros**

DS3 **Administrar el desempeño y la capacidad**

DS4 **Garantizar la continuidad del servicio**

DS5 **Garantizar la seguridad de los sistemas**

DS6 Identificar y asignar costos

DS7 Educar y entrenar a los usuarios

DS8 **Administrar la mesa de servicio y los incidentes**

DS9 **Administrar la configuración**

DS10 **Administrar los problemas**

DS11 **Administrar los datos**

DS12 **Administrar el ambiente físico**

DS13 **Administrar las operaciones**

MONITOREAR Y EVALUAR

ME1 Monitorear y Evaluar el Desempeño de TI

ME2 Monitorear y Evaluar el Control Interno

ME3 Garantizar el Cumplimiento Regulatorio

ME4 Proporcionar Gobierno de TI

Las guías parten de los aspectos articulables de COBIT con ISO 27002. Inician por los Procesos de TI pertenecientes al Dominio de Planeación y Organización (Primer dominio del modelo) y continúa con los procesos de los siguientes dominios continuando el orden que presenta el Modelo.

Para cada Proceso de TI tratado se muestra gráficamente los Recursos de TI involucrados, los Criterios de Información que considera y las Áreas Focales del Gobierno de TI que toca. ***Ver Figura Nº 8.*** A continuación se exponen los Objetivos de Control de COBIT que articulan con los Objetivos de Control de la Norma ISO 27002, los cuales se exponen seguidamente, y cada una de estas exposiciones se cierra con las Recomendaciones Específicas de las Guías de Aseguramiento.

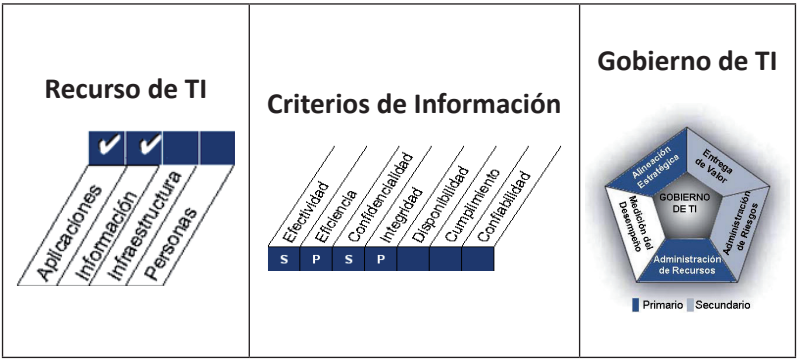


Figura N°8 Recursos de TI involucrados

Siguiendo la normatividad definida por COBIT, los Recursos de TI involucrados en el proceso se encuentran señalados mediante el uso de una marca de chequeo (√),

para los Criterios de la Información a ser considerados se señalan con una letra **P** o con una **S.** Significando cada letra el nivel de importancia **P**rimario o **S**ecundario según el caso.

El pentágono de las áreas focales se manejan con tonalidades, siendo el color oscuro el utilizado para señalar las Áreas de Foco de TI tocadas con importancia Primaria, las más tenues para la importancia Secundaria y las incoloras para las que no tienen importancia para el proceso.

Bibliografía

IT GOVERNANCE INSTITUTE. Marco de Referencia de COBIT 4.1, 2007

ICONTEC. Manual Norma ISO/IEC 27001:2005. Sistema de Gestión de Seguridad de la Información, 2005

ICONTEC. Norma ISO/IEC 27002:2005. Código de Prácticas para la Gestión de Seguridad de la Información, 2005

IT GOVERNANCE INSTITUTE. IT Assurance Guide. Using COBIT

IT GOVERNANCE INSTITUTE. Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

APÉNDICES

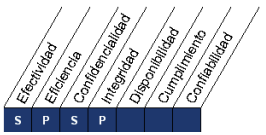
APÉNDICE A

GUÍAS PARA EL DOMINIO DE PLANIFICAR Y ORGANIZAR

PLANEAR Y ORGANIZAR (PO)

PO2 Definir la Arquitectura de la información

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.

Recursos de TI	Criterios de Información	Gobierno de TI
		

PO2.2 Diccionario de Datos Empresarial y Regla de Sintaxis de Datos

Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita compartir elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.

Guías de Aseguramiento

- Pregunte y confirme si las directrices de datos de sintaxis se mantienen.
- Pregunte y confirmar si el diccionario de datos es definido para identificar la redundancia y la incompatibilidad de los datos y que el impacto de cualquier modificación de los datos diccionario y los cambios realizados en el diccionario de datos se comunican efectivamente.
- Los sistemas de aplicación y revisión de diversos proyectos de desarrollo se debe verificar que el diccionario de datos se utiliza para las definiciones de datos.
- Pregunte si se confirman que los altos directivos están de acuerdo sobre el proceso para definir las reglas de la sintaxis de los datos, reglas de validación de datos y reglas de negocio (por ejemplo, la coherencia, integridad, calidad).
- Inspeccione los planes del programa de calidad de los datos, las políticas y procedimientos para evaluar su eficacia.

PO2.3 Esquema de Clasificación de Datos

Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

7.2.1 Directrices de clasificación

Control

La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

Guía de implementación

Las clasificaciones y los controles de protección deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

Las directrices de clasificación deberían incluir convecciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con una política predeterminada de control del acceso.

Debería ser responsabilidad del propietario del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado. La clasificación debería considerar el efecto de suma.

Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

10.7.1 Gestión de medios removibles

Control

Se debería establecer procedimientos para la gestión de los medios removibles.

Guía de implementación

Se debería tener en cuenta las siguientes directrices:

a) Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se deberían hacer irrecuperables.

b) Cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría.

c) Todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.

d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio, también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.

e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente perdida de datos.

f) Las unidades de medios removibles sólo se debería habilitar si existen razones del negocio para hacerlo.

Todos los procedimientos y niveles de automatización deberían estar documentados con claridad.

10.8.1 Políticas y procedimientos para el intercambio de información

Control

Se deberían establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicio de comunicación.

Guía de implementación

Los procedimientos y controles a seguir, cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) Procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.

b) Procedimiento para detección y protección contra código malicioso que se pueden transmitir con el uso de comunicaciones electrónicas.

c) Procedimiento para proteger la información electrónica sensible comunicada que está en forma de adjunto.

d) Políticas o directrices que enfatice el uso aceptable de los servicios de comunicación electrónica.

e) Procedimiento para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.

f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación.

g) Uso de técnicas criptográficas, por ejemplo para proteger la confidencialidad, la integridad y la autenticidad de la información.

h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y reglamentos locales y nacionales correspondientes.

i) No dejar información sensible o critica en los dispositivos de impresión como copiadoras, impresoras y maquinas de facsímil ya que se puede permitir el acceso de personal no autorizado.

j) Controles y restricciones asociados con el envió de servicios de comunicación, como el envió automático de correo electrónico a direcciones de correo externas.

k) Recordar al personal que se deberían tomar precauciones adecuadas como, por ejemplo, no revelar información sensible para evitar que, cuando se hace una llamada telefónica, sea interceptada o escuchada por:

   1. Personas en la cercanía inmediata, particularmente cuando se utiliza teléfonos móviles.

   2. Intercepciones telefónicas o otras formas de escucha no autorizadas mediante el acceso físico al auricular o a la línea telefónica, o usando receptores de exploradores.

   3. Personal al lado del receptor.

l) No dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea.

m) Recordar al personal sobre los problemas de usar maquinas de facsímil a saber:

   1. Creación de acceso no autorizado en los almacenes de mensajes para recuperar los mansajes.

   2. Programación deliberada o accidental de maquinas para enviar mensajes a números específicos.

   3. Envío de documentos y mensajes al número equivocado, bien sea por marcación errónea o por usar el número almacenado erróneamente.

n) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado.

o) Recordar al personal que las maquinas modernas de facsímil y las fotocopiadoras tienen páginas de almacenamiento y caché, en caso de falla en el papel o la transmisión, que se puede imprimir una vez se ha solucionado la falla.

Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

Los servicios de intercambio de información deberían cumplir todos los requisitos legales pertinentes.

11.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) Requisitos de seguridad de las aplicaciones individuales del negocio.

b) Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.

c) Políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información.

d) Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.

e) Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.

f) Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.

g) Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.

h) Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.

i) Requisitos para la autorización formal de las solicitudes de acceso.

j) Requisitos para la revisión periódica de los controles de acceso.

k) Retiro de los derechos de acceso.

Guías de Aseguramiento

- Revisar el sistema de clasificación de datos y verificar que todos los componentes importantes están cubiertos y completado, y que el sistema es razonable en el balance de costo Vs riesgo.
- Esto incluye la propiedad de los datos con los dueños de negocios y la definición de seguridad apropiados en las medidas relacionadas con los niveles de clasificación.
- Verifique que las clasificaciones de seguridad han sido cuestionadas y se confirma con los dueños de negocios a intervalos regulares.

PO3 Determinar la Dirección Tecnológica

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.

Recursos de TI

Criterios de Información

Gobierno de TI

PO3.1Planeación de la Dirección Tecnológica

Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

5.1.2Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos claves para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Éstas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal.

b) Las direcciones o los números telefónicos.

c) La estrategia del negocio.

d) Los lugares, dispositivos y recursos.

e) La legislación.

f) Los contratistas, proveedores y clientes principales.

g) Los procesos existentes, nuevos o retirados.

h) Los riesgos (operativos y financieros).

Guías de Aseguramiento

- Revisar el proceso de las fortalezas, debilidades, oportunidades y amenazas (FODA) de análisis de rendimiento para garantizar la eficacia del proceso (por ejemplo, comprobar si las medidas de el proceso y los cambios realizados en el proceso como resultado de la mejora).
- Confirmar a través de entrevistas con el CIO y otros miembros de la alta dirección de que el apetito por riesgo tecnológico, se ha establecido con base en la la estrategia de negocio.

PO3.3 Monitoreo de Tendencias y Regulaciones Futuras

Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

Guías de Aseguramiento

- Determinar si, por quién y cómo las actuales y las tendencias futuras y los reglamentos son monitoreados (por ejemplo, la evolución tecnológica, actividades de la competencia, cuestiones de infraestructura, los requisitos legales y los cambios reglamentarios medio ambiente, expertos de terceras partes) y si los riesgos relacionados o las oportunidades relacionadas con la creación de valor sean adecuadamente evaluadas.

- Verifique si el resultado de la vigilancia es constante transmitido a los órganos correspondientes (por ejemplo, comité de dirección de TI) y de la táctica de TI y los procesos de planificación de la infraestructura para la acción. EscucharLeer fonéticamente Diccionario - Ver diccionario detalladoEscuchar

- Leer fonéticamente

- Diccionario –

  Ver diccionario detallado

PO3.4 Estándares Tecnológicos

Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal. Se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

10.8.2 Acuerdos para el intercambio

Control

Se deberían establecer acuerdos para intercambio de la información y del software entre la organización y las partes externas.

Guías de implementación

En los acuerdo de intercambio se deberían tomar en consideración las siguientes consideraciones de seguridad:

a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción.

b) Procedimientos para notificar a quien envía la transmisión, el despacho y la recepción.

c) Procedimientos para garantizar la trazabilidad y el no-repudio.

d) Normas técnicas mínimas para el empaquetado y la transmisión.

e) Acuerdos de fideicomiso.

f) Normas para identificar los servicios de mensajería.

g) Responsabilidades y deberes en caso de incidentes de seguridad de la seguridad de la información, como la pérdida de datos.

h) Uso de sistemas acordados de etiquetado de la información sensible o critica, garantizando que el significado de las etiquetas se entiendan inmediatamente y que la información está protegida adecuadamente.

i) Propiedad y responsabilidades para la protección de datos, derechos de copias, conformidad de las licencias de software y consideraciones similares.

j) Normas técnicas para registrar y leer la información y el software.

k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

Se deberían establecer y considerar políticas procedimientos y normas para proteger la información y los medios físicos en tránsito y ellos se deberían referenciar en dichos acuerdos de intercambios.

El contenido sobre la seguridad de cualquier acuerdo debería reflejar la sensibilidad de la información del negocio involucrada.

11.7.2 Trabajo remoto

Control

Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guías de implementación

Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) Seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.

b) El entorno físico de trabajo remoto propuesto.

c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el alcance de comunicación y la sensibilidad del sistema interno.

d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio por ejemplo familiares y amigos.

e) El uso de redes domesticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.

f) Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.

g) El acceso al equipo de propiedad (para verificar la seguridad de la maquina o durante una investigación), el cual puede estar prohibido por la ley.

h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

i) Protección de antivirus y requisitos de firewall.

Las directrices y disposiciones a considerar debería incluir las siguientes:

a) Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.

b) Definición del trabajo que se permite realizar, las horas laborales, la confidencialidad de la información que se conserva y los sistemas y los servicios internos para los cuales el trabajador tiene acceso autorizado.

c) Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.

d) Seguridad física.

e) Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

f) Disposición de soporte y mantenimiento de hardware y software.

g) Disposición de pólizas de seguros.

h) Procedimientos para el respaldo y la continuidad del negocio.

i) Auditoria y monitoreo de seguridad.

j) Revocación de auditoría y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

Guías de Aseguramiento

- Verificar que las normas de la tecnología de la empresa están siendo aprobadas por el Consejo de la arquitectura de TI. Evaluar la eficacia del proceso de comunicación de las normas técnicas para los miembros del personal de TI (por ejemplo, gestores de proyectos, arquitectos de información). Entrevista pertinentes al personal de TI para determinar su conocimiento de las normas técnicas.

- Determinar a partir de la administración de TI que el seguimiento y la evaluación comparativa de los procesos se ponen en marcha para confirmar el cumplimiento de los estándares de tecnología y directrices establecidas.

- Evaluar la documentación técnica de análisis de viabilidad de proyectos seleccionados para evaluar el cumplimiento de estándares de la tecnología empresarial.Diccionario - Ver diccionario detalladoEscuchar

- Leer fonéticamente

- Diccionario –

Ver diccionario detallado

PO3.5 Consejo de Arquitectura de TI

Establecer un comité de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación, y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se vinculan con el PO2 *Definir arquitectura de la información.*

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

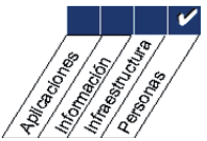
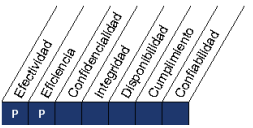
Guías de Aseguramiento

- Revisar las directrices, planes, procesos y actas de las reuniones de la junta arquitectura. Compruebe si ofrecen orientaciones sobre la arquitectura y asesoramiento relacionados de acuerdo con la estrategia de negocio y arquitectura de la información establecida.
- Compruebe si la junta arquitectura se ha planteado el cumplimiento normativo y la continuidad del negocio en sus decisiones.
- Verificar que existan mecanismos que garanticen la detección de incumplimiento de las normas y directrices de la junta la arquitectura dentro del proceso de gestión de proyectos.
- Evaluar el papel de la junta de arquitectura en el seguimiento a través de las correcciones necesarias derivadas de la falta de cumplimiento de las normas en el proceso de gestión de proyectos.Escuchar
- Leer fonéticamente
- Diccionario –

  Ver diccionario detallado

PO4. Definir los Procesos, Organización y Relaciones de TI.

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y uno ó más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.

Recursos de TI	Criterios de Información	Gobierno de TI
		

PO4.3 Comité Directivo de TI

Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:

- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa.
- Dar seguimiento al estatus de los proyectos y resolver los conflictos de recursos.
- Monitorear los niveles de servicio y las mejoras del servicio.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

Guías de Aseguramiento

- Pregunte y confirme si la carta, el alcance, objetivos, miembros, funciones, responsabilidades, etc., del resultado del comité directivo de TI en la aplicación adecuada de la dirección estratégica de TI de la empresa.
- Inspeccione los documentos tales como actas de reuniones y la carta del comité de dirección de TI para identificar a los participantes involucrados en la comisión, sus funciones de trabajo respectivos y la relación de informes de la comisión a la dirección ejecutiva (por ejemplo, determinar la priorización de las TI programas habilitados para la inversión, el estado de la pista de los proyectos, y supervisar los niveles de servicio y mejoras en el servicio).
- Preguntar y confirmar con la gestión empresarial para garantizar que la empresa lleva un papel activo en la labor del comité de dirección de TI y gestión debidamente consultados.

PO4.4 Ubicación Organizacional de la Función de TI

Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.1.3 Asignación de responsabilidades para la seguridad de la información.

Control

Se debería definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

Las asignaciones de responsabilidades para la seguridad de la información se debería realizar de acuerdo cao la política de seguridad de la información (punto 5) se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidad de seguridad asignada pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsabilidad y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) Los activos y los proceso de seguridad asociados con cada sistema particular se debería identificar y definir claramente.

b) Se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar estas responsabilidades.

c) se debería definir y documentar claramente los niveles de autorización.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

Guías de Aseguramiento

a) Pregunte y confirme si la función de TI es:

- Bajo la dirección de un CIO o función similar, de los cuales la autoridad, responsabilidad, rendición de cuentas y presentación de informes de línea son proporcionales a la importancia de las TI en la empresa.
- Definición y organizado de tal manera que los grupos de usuarios individuales o departamentos no pueden ejercer una influencia indebida sobre la función de TI y afectar las prioridades acordadas por el comité de estrategia de TI y comité de dirección.
- Con recursos adecuados (por ejemplo, la dotación de personal, contingente, el presupuesto) para permitir la aplicación y gestión adecuada de las soluciones de TI y servicios para apoyar el negocio y permitir a las relaciones con la empresa.
- Ver diccionario detallado

PO4.5 Estructura Organizacional

Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

Guías de Aseguramiento

Pregunte y confirme si:

- Las revisiones periódicas se realizan por el impacto de los cambios organizativos que afectan a la organización en general y la estructura de la función de TI en sí.
- La organización de TI tiene acuerdos flexibles de recursos, tales como el uso de contratistas externos y las disposiciones sobre flexibilidad de servicios a terceros, para apoyar a las cambiantes necesidades empresariales.

PO4.6 Establecimiento de Roles y Responsabilidades

Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definían las responsabilidades y rendición de cuentas para alcanzar las necesidades del negocio.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.1.3 Asignación de responsabilidades para la seguridad de la información.

Control

Se debería definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

Las asignaciones de responsabilidades para la seguridad de la información se debería realizar de acuerdo cao la política de seguridad de la información se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidad de seguridad asignada pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsabilidad y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) Los activos y los proceso de seguridad asociados con cada sistema particular se debería identificar y definir claramente.

b) Se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar estas responsabilidades.

b) Se debería definir y documentar claramente los niveles de autorización.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como “necesidad de conocer”).

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.1.2 Selección

Control

Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Guías de implementación

En las revisiones de verificación se deberían tener en cuenta la legislación pertinente a la privacidad, la protección de datos personales y / o el empleo y cuando se permite, debería incluir lo siguiente:

a) Disponibilidad de referencia de comportamiento satisfactorio, por ejemplo una laboral y otra personal.

b) Una verificación (para determinar la totalidad y exactitud) de la hoja de vida del candidato.

c) Confirmación de las calificaciones profesionales y académicas declaradas.

d) Verificación de la identidad independiente (pasaporte o documento similar)

e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible, como por ejemplo información financiera o de alta confidencialidad, la organización debería considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y las limitaciones para las revisiones de verificación, por ejemplo quien es elegible para seleccionar al personal y cómo, cuándo y por qué se realizan las verificaciones.

También deberían llevar a cabo un proceso de selección para los contratistas y los usuarios de terceras partes. Cuando los contratistas son suministrados por una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para la selección y los procedimientos de notificación que es necesario seguir si la selección no se ha completado o si los resultados arrojan dudas o preocupación. De la misma manera, el acuerdo de la tercera parte debería especificar claramente todas las responsabilidades y los procedimientos de la notificación para la selección.

Informar sobre todos los candidatos que se consideran para los cargos dentro de la organización se debería recolectar y manejar según la legislación adecuada existente en la jurisdicción correspondiente.

Dependiendo de la legislación que se aplique, se debería informar con anticipación a los candidatos sobre las actividades de selección.

8.1.3 Términos y condiciones laborales

Control

Como parte de la obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual deber establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

Guías de implementación

Los términos y condiciones laborales deberían refleja la política de seguridad de la organización, además deberían aclarar y establecer:

a) Que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a la información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información.

b) Los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o legislación sobre protección de datos.

c) Responsabilidades para la clasificación de la información y la gestión de los activos asociados con sistemas y servicios de información manejados por el empleado, el contratista o usuario de tercera parte.

d) Responsabilidades del empleado, contratista o usuario de tercera parte para el manejo de información recibida de otras empresas o de partes externas.

e) Responsabilidades de la organización para el manejo de la información personal, incluyendo la información personal creada como resultado o durante el contrato laboral con la organización.

f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio.

g) Acciones a tomar si el empleado, contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

La organización debería garantizar que los empleados, los contratistas y los usuarios de terceras partes están de acuerdo con los términos y condiciones respecto a la seguridad de la información según la naturaleza del acceso que tendrán a los activos de la organización asociado con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones laborales deberían durante un periodo definido después de la terminación del contrato laboral (8.3).

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

Guías de Aseguramiento

- Pregunte y confirme si:

✓ Cada tarea de TI se ha formalizado mediante la revisión de la documentación y determinar si son descripciones de las tareas regulares, y como se requiere.

✓ El papel se le ha asignado al personal de TI con las correspondientes tareas de TI. Evaluar si el personal entiende el papel y las tareas que se han asignado, y que las tareas se están llevando a cabo.

- ✓ Rendir cuentas y responsabilidades se han asignado y las funciones (roles). Verificar mediante la inspección de las descripciones de puestos, cartas, etc., que cada función tiene la rendición de cuentas necesarias y responsabilidades para ejecutar la función.
- ✓ El personal de TI se les ha informado de sus funciones o roles. Evaluar si los cambios se comunican al personal de TI y si los cambios se están aplicando.
- ✓ Los directivos periódicamente confirmar la exactitud de las descripciones de papel. revisar las descripciones de papel para determinar si reflejan con precisión las funciones de los miembros del equipo.
- ✓ Papel de las descripciones del esquema metas y objetivos esenciales e incluir medidas SMARRT.
- ✓ Medidas SMARRT se utilizan en las evaluaciones de desempeño del personal.
- ✓ Todas las descripciones de papel en la organización incluyen responsabilidades en relación con los sistemas de información, control interno y la seguridad.
- ✓ Gestión de los trenes de los miembros del personal regularmente en sus funciones. Entrevista personal de los miembros para determinar si el conocimiento de la función se ha comunicado y comprendido.

- Para determinar si los empleados cuentan con políticas de toda la empresa y departamentales, y los procedimientos, se debe revisar el:
- ✓ El reconocimiento anual de la política.
- ✓ HR registros que indiquen si los empleados se les proporcionó la documentación durante la orientación política de nuevas contrataciones.
- ✓ Registro de empleados de formación

PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento

Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.1.3 Asignación de responsabilidades para la seguridad de la información.

Control

Se debería definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

Las asignaciones de responsabilidades para la seguridad de la información se debería realizar de acuerdo cao la política de seguridad de la información (punto 5) se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidad de seguridad asignada pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsabilidad y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) Los activos y los proceso de seguridad asociados con cada sistema particular se debería identificar y definir claramente.

b) Se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar estas responsabilidades.

c) Se debería definir y documentar claramente los niveles de autorización.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, contratistas y los usuarios de terceras partes:

a) Están adecuadamente informado sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se le otorgue acceso a la información o sistemas de información sensible.

b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.

c) Estén motivados para cumplir las políticas de seguridad de la organización.

d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización, teniendo en cuenta el siguiente ítem.

e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen las políticas de seguridad de la información de la organización y los métodos apropiados de trabajo.

f) Sigan teniendo las calificaciones y habilidades apropiadas.

8.2.3 Proceso disciplinario

Control

Debería existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.

Guía de implementación

No se recomienda iniciar el proceso disciplinario antes de verificar que se ha presentado la violación de la seguridad.

El proceso disciplinario formal debería garantizar el tratamiento imparcial y correcto para los empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal debería brindar una respuesta gradual que considere factores tales como la naturaleza y la gravedad de la violación y su impacto en el negocio, si es la primera ofensa o se repite, si el violador está capacitado adecuadamente, la legislación correspondiente, los contratos de negocio y otros factores, según el caso. En los casos graves de mala conducta el proceso debería permitir el retiro instantáneo de las funciones, los derechos de acceso y los privilegios y el acompañamiento inmediato fuera de las instalaciones, si es necesario.

15.1.1 Identificación de la legislación aplicable

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

Guía de implementación

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implementación

Se deberían tomar en consideración las siguientes directrices para proteger todo el material que se pueda considerar propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.

b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

c) Mantener la concientización de sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que lo viole.

d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

f) Implementar controles para asegurar que no se excede al número máximo de usuarios permitidos.

g) Verificar que únicamente se instalan software autorizado y productos con licencias.

h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar las herramientas de auditoría adecuada.

k) Cumplir los términos y condiciones para el software y la información obtenido de redes públicas.

l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.

m) No copiar total ni parcialmente libros, archivos, informe ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

15.1.3 Protección de los registros de la organización

Control

Los requisitos importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios y contractuales y del negocio.

Guía de implementación

Los registros se deberían clasificar en tipos de registros, por ejemplo registro de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno con los detalles de los periodos de retención y los tipos de medio de almacenamientos como papel, microfichas, medios magnéticos, ópticos, etc. Todo el material relacionado con claves criptográficas y programas asociados a los archivos encriptados o firmas digitales, también se debería almacenar para permitir el descifrado de los registros durante el periodo tiempo durante el cual se retienen los registros.

Es conveniente tomar en consideración la posibilidad de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberían implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso del papel y microfichas.

Al seleccionar los medios de almacenamiento electrónico, se deberían incluir los procedimientos para garantizar la capacidad de acceso a los datos (facilita tanto el medio como el formato) durante todo el periodo de retención para salvaguardar contra pérdida debido a cambio en la tecnología futura.

Los sistemas de almacenamiento de datos de deberían seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.

El sistema de almacenamiento y manipulación debería garantizar la identificación de los registros y su periodo de retención tal como se define en los reglamentos o la legislación nacional o regional, si se aplica. Este sistema debería permitir la destrucción adecuada de los registros después de este periodo, si la organización no los necesita.

Para cumplir estos objetivos de salvaguardia de registros, la organización debería seguir los siguientes aspectos:

a) Se deberían publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registro e información.

b) Es conveniente publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención.

c) Se recomienda conservar un inventario de las fuentes de información clave.

d) Se deberían implementar los controles apropiado para proteger los registros y la información contra pérdida, destrucción y falsificación.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

15.1.6 Reglamento de los controles criptográficos

Control

Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

Guía de implementación

Se recomienda tener presentes los siguientes elementos para el cumplimiento con acuerdos, leyes y reglamentos pertinentes:

a) Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de las funciones criptográficas.

b) Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.

c) Restricciones al uso de encriptación.

d) Métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

Se debería buscar asesoría legal para garantizar el cumplimiento con las leyes y los reglamentos nacionales. Antes de desplazar la información encriptada o los controles criptográficos a otros países, se debería tener asesoría legal.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

Pregunte y confirme si:

- La alta dirección ha establecido que toda la organización, el personal maneja adecuadamente la función de seguridad de información y gestión de riesgo global rendición de cuentas para la seguridad de información y gestión del riesgo. Verificar mediante entrevistas a personal clave que la línea de información de la gestión del riesgo y la función de seguridad de la información es tal que puede diseñar, aplicar y, en relación con la gestión de la línea, hacer cumplir la gestión de riesgos de la organización y las políticas de seguridad de la información, normas y procedimientos efectivamente.

- Funciones y responsabilidades para la gestión del riesgo y la función de seguridad de la información se han formalizado y documentado.

- Las responsabilidades se han asignado a los miembros del personal debidamente cualificado y experimentado y, en el caso de la seguridad de la información, se realiza bajo la dirección de un oficial de seguridad de la información.

- Las necesidades de recursos en relación con la gestión de riesgos y seguridad de la información se han evaluado periódicamente por la administración para asegurar que se asignen recursos suficientes para satisfacer las necesidades de la empresa.

- Un proceso en marcha para obtener orientación sobre la administración superior del perfil de riesgo y la aceptación de riesgos residuales significativos. Verifique que funciona correctamente mediante el examen de situaciones recientes.

PO4.9 Propiedad de Datos y de Sistemas

Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los dueños toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

6.1.3 Asignación de responsabilidades para la seguridad de la información.

Control

Se debería definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

Las asignaciones de responsabilidades para la seguridad de la información se debería realizar de acuerdo cao la política de seguridad de la información se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidad de seguridad asignada pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsabilidad y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) Los activos y los proceso de seguridad asociados con cada sistema particular se debería identificar y definir claramente.

b) Se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar estas responsabilidades.

c) Se debería definir y documentar claramente los niveles de autorización.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

7.1.2 Propietario de los activos

Control

Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser propietario de una parte designada de la organización.

Guía de implementación

El propietario del activo debe ser responsable de:

a) Garantizar que la información y los activos asociados con los servicios de procesamiento de la información de clasifican adecuadamente.

b) Definir y revisar periódicamente las restricciones y clasificaciones de los accesos.

La propiedad se puede asignar a:

a) Un proceso de negocio.

b) Un conjunto definido de actividades.

c) Una aplicación.

d) Un conjunto definido de datos.

9.2.5 Seguridad de los equipos fuera de las instalaciones

Control

Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Guía de implementación

Independientemente del propietario, la dirección debería autorizar el uso del equipo de procesamiento de información fuera de las instalaciones de la organización.

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo fuera de las instalaciones:

a) El equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes.

b) Se debería observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra explosión a campos electromagnéticos fuertes.

c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgo y controles adecuados que se aplican de forma idónea, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina (ISO/IEC 18028, Seguridad de la red).

d) Se debería establecer el cubrimiento adecuado del seguro para proteger el equipo fuera de las instalaciones.

Los riesgos de seguridad, como daño, robo o escuchas no autorizadas pueden variar considerablemente entre los lugares y se deberían tener en cuenta para determinar los controles más apropiados.

Guías de Aseguramiento

• Preguntar y confirmar si se ha desarrollado una política para la propiedad de clasificación y sistema de datos y que también este comunicada.

• Validar que la política se ha aplicado a sistemas de aplicaciones principales y la arquitectura de empresa y la comunicación de datos internos y externos.

• Verificar que la política para la propiedad de clasificación y sistema de datos es compatible con la protección de los activos de información, permite la eficacia de la prestación y el uso de aplicaciones de negocios y facilita la toma de decisiones de seguridad eficaces.

• Observar el proceso para registrar y mantener la propiedad del sistema y la clasificación de datos y evaluar si el proceso está siendo aplicado sistemáticamente.

PO4.10 Supervisión

Implementar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las deberían llevar a cabo otros organismos de la dirección o un solo director.

6.1.3 Asignación de responsabilidades para la seguridad de la información

Control

Se debería definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

Las asignaciones de responsabilidades para la seguridad de la información se debería realizar de acuerdo cao la política de seguridad de la información se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se debería definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidad de seguridad asignada pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsabilidad y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) Los activos y los proceso de seguridad asociados con cada sistema particular se debería identificar y definir claramente.

b) Se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar estas responsabilidades.

c) Se debería definir y documentar claramente los niveles de autorización.

7.1.3 Uso aceptable de los activos

Control

Se debería identificar, documentar e implementar las reglas sobre el uso de aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo:

a) Reglas para el uso del correo electrónico y el internet.

b) Directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de terceras partes que utilizan o tienen acceso a los activos de la organización deberían estar consientes de los limites que existen para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Deberían ser responsables del uso para que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

8.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, contratistas y los usuarios de terceras partes:

a) Están adecuadamente informado sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se le otorgue acceso a la información o sistemas de información sensible.

b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.

c) Estén motivados para cumplir las políticas de seguridad de la organización.

d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización, teniendo en cuenta el siguiente ítem.

e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen las políticas de seguridad de la información de la organización y los métodos apropiados de trabajo.

f) Sigan teniendo las calificaciones y habilidades apropiadas.

Guías de Aseguramiento

• Confirmar a través de entrevistas que las prácticas de supervisión han sido establecidas, incluida la orientación y formación para las revisiones de rendimiento.

• Los registros de revisión para evaluar la frecuencia y el alcance de las revisiones de control y evaluaciones de personal.

• Evaluar si las revisiones tienen un conjunto sólido de las expectativas de desempeño y criterios de desempeño.

• Pregunte si, y confirmar que los resultados de los exámenes de supervisión y evaluación de los funcionarios estén adecuadamente escalonada, comunicados y seguimiento.

PO4.11 Segregación de Funciones

Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

8.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, contratistas y los usuarios de terceras partes:

a) Están adecuadamente informado sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se le otorgue acceso a la información o sistemas de información sensible.

b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.

c) Estén motivados para cumplir las políticas de seguridad de la organización.

d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización, teniendo en cuenta el siguiente ítem.

e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen las políticas de seguridad de la información de la organización y los métodos apropiados de trabajo.

f) Sigan teniendo las calificaciones y habilidades apropiadas.

10.1.3 Distribución (Segregación) de funciones

Control

Las funciones y las áreas de responsabilidad se deberían distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

Guías de implementación

La distribución de funciones es un método para reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se debería tener cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento se debería separar de su autorización. Es conveniente considerar la posibilidad de complicidad al diseñar los controles.

Las organizaciones pequeñas pueden encontrar difícil de lograr la distribución de funciones, pero el principio se debería aplicar en la medida de lo posible y viable. Siempre que haya dificultad para la distribución, se deberían considerar otros controles como monitoreo de actividades, registros de auditoría y supervisión por la dirección. Es importante que la auditoria de seguridad siga siendo independiente.

10.1.4 Separación de la instalaciones de desarrollo, ensayo y operación

Control

Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

Guías de implementación

Se debería identificar el grado de separación entre los ambientes operativos, de prueba y de desarrollo que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Se deberían tener presente los siguientes elementos:

a) Se recomienda definir y documentar las reglas para la transparencia de software del estado de desarrollo al operativo.

b) El software de desarrollo y el operativo se deberían ejecutar de diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.

c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando nos se requiera.

d) El ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible.

e) Los usuarios deberían emplear perfiles de usuarios diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error.

f) Los datos sensibles no se deberían copiar en el entorno del sistema de prueba.

10.6.1 Controles de las redes

Control

Las redes de deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

Guías de implementación

Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa por las redes debería estar separada de la operaciones de computador, según sea apropiado (**10.1.3 Distribución (Segregación) de funciones** de la cual se hace referencia en el primer ítem de la guía).

b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remostos, incluyendo los equipos en áreas de usuario.

c) Es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas; también se puede requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.

d) Se debería aplicar el registro y el monitoreo adecuado para permitir el registro de acciones de seguridad pertinente.

e) Se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

Guías de Aseguramiento

- Preguntar y confirmar si se han establecido normas para aplicar y garantizar la adecuada separación de funciones y que estas normas son revisadas y cambiado según sea necesario.
- Evaluar si se han aplicado las normas en la asignación de roles y responsabilidades.
- Preguntar si y confirme que existe un proceso para identificar posiciones críticas y procesos que deberán ser sometidos a la separación de funciones.

PO4.14 Políticas y procedimientos para personal contratado

Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa de tal manera que se logren los requerimientos contractuales acordados.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

   1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

   2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

   3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

   4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

3) Proceso de autorización para los privilegios y el acceso de usuario.

4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

   1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

   2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

   3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

9.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) El personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida.

b) Se debería evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.

c) Las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente.

d) No se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información

Control

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

Guía de implementación

La dirección debería aprobar el uso de los servicios de procesamiento de información. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio.

Guías de Aseguramiento

- Revise las políticas y procedimientos que describe cuándo, cómo y qué tipo de trabajo pueden ser subcontratadas o manejadas por un tercero, y determinar si se están aplicando.

- Revise las políticas y procedimientos de seguridad de la información responsabilidades de los contratistas, y evaluar a través de la investigación si se están siguiendo (por ejemplo, verificar que antecedentes se llevan a cabo, física y lógica de los requisitos de control de acceso, que la identificación personal es segura, y los contratistas se asesoran que la gestión se reserva el derecho de supervisar e inspeccionar todo el uso de los recursos de TI, incluyendo el correo electrónico, las comunicaciones de voz, y todos los programas y archivos de datos).

- Revisar las políticas y procedimientos para la selección de un contratista, y evaluar si éstos se están aplicando.

PO4.15 Relaciones

Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI, tales como el consejo directivo, ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo de cumplimiento corporativo, los contratistas externos y la gerencia externa (offsite).

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

6.1.7 Contactos con grupos de interés especiales

Control

Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

Guía de implementación

La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

a) Mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.

b) Garantizar que la comprensión del entorno de seguridad de la información es actual y completa.

c) Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.

d) Obtener acceso a asesoría especializada sobre seguridad de la información.

e) Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

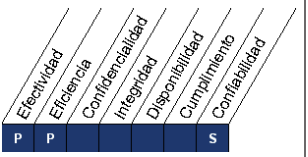
f) Suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información.

Guías de Aseguramiento

- Pregunte y confirme si el proceso para identificar a los interesados ha sido definido y qué canal de comunicaciones se han establecidos para cada uno.
- Verificar a través de entrevistas con los principales interesados su satisfacción con sus comunicaciones, la eficacia de TI de las comunicaciones y la adecuación con que a las partes interesadas se está tratando.

PO5Administrar la Inversión en TI.

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias. El proceso fomenta la asociación entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.

Recurso de TI	Criterios de Información	Gobierno de TI
		

PO5.3 Proceso Presupuestal

Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y de los presupuestos de programas individuales.

5.1.2 Revisión de la política de seguridad de la información

Control

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

a) Retroalimentación de las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimiento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

a) Mejora del enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y / o responsabilidades.

Es recomendable mantener un registro de la revisión por la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

Guías de Aseguramiento

- Pregunte y confirme si se ha aplicado una metodología para establecer, cambiar, aprobar y comunicar un formal presupuesto de TI.

- Revisar el presupuesto de TI para verificar que si son los elementos pertinentes (por ejemplo, fuentes autorizadas de la financiación, los costes de recursos internos, los costes de terceros, de capital y gastos operativos) se tienen en cuenta al crear el presupuesto.
- Pregunte y confirme si las contingencias presupuestarias se han identificado y justificado para estas contingencias que ha sido aprobada.
- Verificar que la eficacia del proceso de presupuesto se controla (la asignación de costos, asignación de costos de servicios y análisis de variación del presupuesto), y los informes de revisión para verificar que las lecciones aprendidas se registran para hacer el presupuesto futuro más exacto y fiable.
- Pregunte y confirme si las personas involucradas en el proceso presupuestario (por ejemplo, procesos, servicios y propietarios de programas, gestores de activos) dan las instrucciones adecuadas.
- Pregunte y confirme si hay un proceso de creación del presupuesto aprobado y coherente (por ejemplo, revisar el presupuesto de los planes, tomar decisiones sobre las asignaciones presupuestarias, y recopilar y comunicar los presupuestos generales de IT, la asignación del costo del proyecto, la asignación de costos de los servicios y el análisis de variación del presupuesto).

PO5.4 Administración de Costos de TI

Implementar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, éstas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

5.1.2 Revisión de la política de seguridad de la información

Control

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

a) Retroalimentación de las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimiento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

a) Mejora del enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y / o responsabilidades.

Es recomendable mantener un registro de la revisión por la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

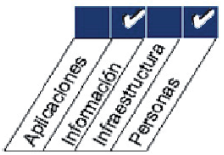
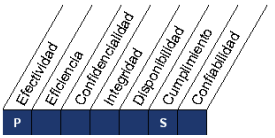
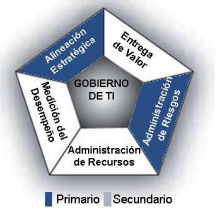
La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

Guías de Aseguramiento

- Pregunte y confirmar se ha definido un marco para la gestión de TI relacionados con los costes de TI y que son adecuadas y debidamente clasificadas las categorías del gasto global.
- Confirme que no hay una adecuada independencia entre los individuos que capturar, analizar y reportar información financiera, y los titulares de presupuesto de TI.
- Revisión de los plazos establecidos para determinar si están alineados con el presupuesto y los requisitos de contabilidad y, dentro de los proyectos de TI, ya sea que se estructuran de acuerdo con el calendario los resultados finales.
- Pregunte y confirme si, se ha definido el método que recopila datos para identificar las desviaciones especificadas.
- Verificar que los sistemas de recolección de datos han sido identificados.
- Determinar si la información proporcionada por los sistemas es completa, precisa y coherente.
- Determinar la forma de cómo se consolida en función los costos relacionados con la información, la forma en que se presenta en diversos niveles en la organización y para los interesados, y si ayuda a permitir la identificación oportuna de medidas correctivas necesarias.

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.

Recurso de TI	Criterios de Información	Gobierno de TI
		

PO6.1 Ambiente de Políticas y de Control

Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras administra riesgos significativos, fomenta la colaboración entre divisiones y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

   incluyendo los siguientes:

   1) cumplimiento de los requisitos legales, reglamentarios y contractuales;

   2) requisitos de educación, formación y concientización sobre seguridad;

   3) gestión de la continuidad del negocio;

   4) consecuencias de las violaciones de la política de seguridad;

e) Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

13.2.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Guía de implementación

Además del reporte de los eventos y las debilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades se debería emplear para detectar los incidentes de la seguridad de la información. Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de los incidentes de seguridad de la información:

a) Es conveniente instaurar procedimientos para manejar los diferentes tipos de incidentes

   de seguridad de la información, incluyendo:

   1) Fallas en el sistema de información y pérdida del servicio.

   2) Códigos maliciosos.

   3) Negación del servicio.

   4) Errores producidos por datos del negocio, sean incompletos o inexactos.

   5) Violaciones de la confidencialidad y la integridad.

   6) Uso inadecuado de los sistemas de información.

b) Además de los planes normales de contingencia, los procedimientos también deberían comprender:

   1) El análisis y la identificación de la causa del incidente.

2) La contención.

3) La planificación e implementación de la acción correctiva para evitar la recurrencia, si es necesario.

4) La comunicación con aquellos afectados o implicados con la recuperación después del incidente.

5) El reporte de la acción a la autoridad apropiada.

c) Se deberían recolectar y asegurar los rastros para auditoría y la evidencia similar, según sea apropiado para:

1) El análisis de los problemas internos.

2) El uso de evidencia forense con respecto a la posible violación del contrato o del requisito reglamentario o en caso de juicios criminales o civiles, por ejemplo, según la legislación sobre uso inadecuado del computador o sobre protección de datos.

3) La negociación para la compensación proveniente de los proveedores de software y servicios.

d) La acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada; los procedimientos deberían garantizar que:

1) Únicamente el personal claramente identificado y autorizado tiene acceso a los sistemas y datos activos.

2) Todas las acciones de emergencia están documentadas en detalle.

3) La acción de emergencia se reporta a la dirección y se revisa de manera ordenada.

4) La integridad de los sistemas y controles del negocio se confirma con retraso mínimo.

Los objetivos de la gestión de los incidentes de seguridad de la información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de seguridad de la información.

Guías de Aseguramiento

- Pregunte y confirme si, la existencia de un oficial de comunicación "tono en la parte superior" (por ejemplo, el boletín CIO o de la intranet, correos electrónicos periódicos, TI la visión y principios rectores) que permita definir y gestionar los riesgos de TI y la infraestructura de control y garantizar que se alinee con el riesgo general de la organización y el medio ambiente de control.

- Determinar si la rendición de cuentas y la responsabilidad han sido asignadas a los individuos para establecer y reforzar las comunicaciones de la cultura de control.

- Confirmar la existencia de políticas y prácticas para apoyar el ambiente de control (por ejemplo, las políticas de uso aceptable, verificación de antecedentes).

- Inspeccione los títulos de formación periódica de sensibilización sobre estas políticas y prácticas.

- Determinar si existe un proceso de forma periódica (al menos anualmente) que calcule de nuevo la adecuación del entorno de control y tolerancia al riesgo para asegurarse de que está alineada con el entorno cambiante de la organización.

- Pregunte y confirme si, las políticas de recursos humanos (por ejemplo, verificación de antecedentes a los solicitantes de empleo, cursos de sensibilización a las nuevas contrataciones, firmado el código de la documentación conducta, las consecuencias apropiadas para la conducta no ética) apoya el control de TI al medio ambiente.

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI

Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y el control que se alinee con la política de TI, el ambiente de control y el marco de trabajo de riesgo y control de la empresa.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

incluyendo los siguientes:

1) Cumplimiento de los requisitos legales, reglamentarios y contractuales.

2) Requisitos de educación, formación y concientización sobre seguridad.

3) Gestión de la continuidad del negocio.

4) Consecuencias de las violaciones de la política de seguridad.

e) Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

6.2.2 Abordaje de la seguridad cuando se trata con los clientes

Control

Todos los requisitos de seguridad identificados se deberían abordar antes de dar acceso a los clientes a los activos o la información de la organización.

Guía de implementación

Los siguientes términos se deberían considerar para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización (dependiendo del tipo y la extensión de dicho acceso, no se podrían aplicar todos ellos):

a) Protección de activos, incluyendo:

1) Procedimientos para proteger los activos de la organización, incluyendo información y software, y gestión de las vulnerabilidades conocidas.

2) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de datos.

3) Integridad.

4) Restricciones a la copia y la divulgación de la información.

b) Descripción del producto o servicio que se va proveer.

c) Las diversas razones, requisitos y beneficios del acceso del cliente.

d) Política de control del acceso, incluyendo:

1) Métodos de acceso permitido y control y uso de identificadores únicos tales como la identificación del usuario (ID) y las contraseñas.

2) Proceso de autorización para los privilegios y el acceso de los usuarios.

3) Declaración de que el acceso que no se autorice explícitamente está prohibido.

4) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

e) Convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de detalles personales), incidentes de seguridad de la información y violaciones de la seguridad.

f) Descripción de cada servicio que va a estar disponible.

g) La meta del nivel de servicio y los niveles inaceptables de servicio.

h) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

i) Las respectivas responsabilidades civiles de la organización y del cliente.

j) Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con clientes en otros países.

k) Derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.

7.1.3 Uso aceptable de los activos

Control

Se debería identificar, documentar e implementar las reglas sobre el uso de aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo:

a) Reglas para el uso del correo electrónico y el internet.

b) Directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de terceras partes que utilizan o tienen acceso a los activos de la organización deberían estar consientes de los limites que existen para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Deberían ser responsables del uso para que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

8.3.2 Devolución de activos

Control

Todos los empleados, contratistas o usuarios de terceras partes deberían devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.

Guía de implementación

Se debería formalizar el proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la organización tales como los dispositivos de cómputo móviles, las tarjetas de crédito, las tarjetas de acceso, el software, los manuales y la información almacenada en medios electrónicos.

Cuando un empleado, contratista o usuario de terceras partes adquiere equipo de la organización o utiliza su propio equipo, se deberían seguir los procedimientos para garantizar que toda la información pertinente se transfiere a la organización y se elimina con seguridad de tal equipo.

Cuando un empleado, contratista o usuario de terceras partes tiene un conocimiento que es importante para la continuación de las operaciones, esa información debería estar documentada y transferirse a la organización.

9.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) El personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida.

b) Se debería evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.

c) Las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente.

d) No se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.

9.2.7 Retiro de activos

Control

Ningún equipo, información ni software se deberían retirar sin autorización previa.

Guía de implementación

Se recomienda tener presentes las siguientes directrices:

a) Ni los equipos, ni la información, tampoco el software se deberían retirar sin autorización previa.

b) Los empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir retirar activos deberían estar claramente identificados.

c) Se recomienda establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de devolución.

d) Cuando sea necesario y adecuado, se debería registrar que el equipo ha sido retirado y se debe registrar cuando fue devuelto.

10.7.3 Procedimientos para el manejo de la información

Control

Se deberían establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

Guía de implementación

Se deberían elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación. Se deberían considerar los siguientes elementos:

a) Manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.

b) Restricciones de acceso para evitar el acceso de personal no autorizado.

c) Mantenimiento de un registro formal de los receptores autorizados de los datos.

d) Garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida.

e) Protección, según su nivel de sensibilidad, de los datos de la memoria temporal que esperan su ejecución.

f) Almacenamiento de los medios según las especificaciones del fabricante.

g) Mantenimiento de la distribución de datos en un mínimo.

h) Rotulado claro de todas las copias de los medios para la autenticación del receptor autorizado.

i) Revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

10.8.1 Políticas y procedimientos para el intercambio de información

Control

Se deberían establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicio de comunicación.

Guía de implementación

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) Procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.

b) Procedimiento para detección y protección contra código malicioso que se pueden transmitir con el uso de comunicaciones electrónicas.

c) Procedimiento para proteger la información electrónica sensible comunicada que está en forma de adjunto.

d) Políticas o directrices que enfatice el uso aceptable de los servicios de comunicación electrónica.

e) Procedimiento para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.

f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación.

g) Uso de técnicas criptográficas, por ejemplo para proteger la confidencialidad, la integridad y la autenticidad de la información.

h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y reglamentos locales y nacionales correspondientes.

i) No dejar información sensible o critica en los dispositivos de impresión como copiadoras, impresoras y maquinas de facsímil ya que se puede permitir el acceso de personal no autorizado.

j) Controles y restricciones asociados con el envió de servicios de comunicación, como el envió automático de correo electrónico a direcciones de correo externas.

k) Recordar al personal que se deberían tomar precauciones adecuadas como, por ejemplo, no revelar información sensible para evitar que, cuando se hace una llamada telefónica, sea interceptada o escuchada por:

    1. Personas en la cercanía inmediata, particularmente cuando se utiliza teléfonos móviles.

    2. Intercepciones telefónicas o otras formas de escucha no autorizadas mediante el acceso físico al auricular o a la línea telefónica, o usando receptores de exploradores.

    3. Personal al lado del receptor.

l) No dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea.

m) Recordar al personal sobre los problemas de usar maquinas de facsímil a saber:

    1. Creación de acceso no autorizado en los almacenes de mensajes para recuperar los mansajes.

    2. Programación deliberada o accidental de maquinas para enviar mensajes a números específicos.

3. Envió de documentos y mensajes al número equivocado, bien sea por marcación errónea o por usar el número almacenado erróneamente.

n) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado.

o) Recordar al personal que las maquinas modernas de facsímil y las fotocopiadoras tienen páginas de almacenamiento y caché, en caso de falla en el papel o la transmisión, que se puede imprimir una vez se ha solucionado la falla.

Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

Los servicios de intercambio de información deberían cumplir todos los requisitos legales pertinentes.

10.9.3 Información disponible al público

Control

La integridad de la información que se pone a disposición en un sistema de acceso público debería estar protegida para evitar la modificación no autorizada.

Guía de implementación

El software, los datos y otra información que requiere un nivel alto de integridad que se pone a disposición en sistemas públicos se debería proteger con mecanismos apropiados como firmas digitales. Los sistemas de acceso público se deberían probar frente a debilidades y fallas antes de que la información esté disponible.

Debería existir un proceso formal de aprobación previo a que la información esté disponible al público. Además, todas las entradas suministradas desde el exterior del sistema se deberían verificar y aprobar.

Los sistemas electrónicos de editorial, especialmente aquellos que permiten retroalimentación y entrada directa de información, se deberían controlar cuidadosamente de modo que:

a) La información se obtenga de conformidad con toda la legislación sobre protección de datos.

b) La entrada de información hacia y procesada por el sistema editorial se procese completa y exactamente de forma oportuna.

c) La información sensible estará protegida durante la recolección, el procesamiento y el almacenamiento.

d) El acceso al sistema editorial no permite acceso involuntario a redes a las cuales se conecta el sistema.

11.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) Requisitos de seguridad de las aplicaciones individuales del negocio.

b) Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.

c) Políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información.

d) Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.

e) Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.

f) Perfiles estándar de acceso de usuario para funciones laborales comunes en laorganización.

g) Gestión de los derechos de acceso en un entorno distribuido y con red que reconozcatodos los tipos de conexiones posibles.

h) Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso,autorización del acceso, administración del acceso.

i) Requisitos para la autorización formal de las solicitudes de acceso.

j) Requisitos para la revisión periódica de los controles de acceso.

k) Retiro de los derechos de acceso.

11.3.1 Uso de contraseñas

Control

Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

Guía de implementación

Todos los usuarios deberían:

a) Mantener la confidencialidad de las contraseñas.

b) Evitar conservar registros (por ejemplo en papel, archivos de software o dispositivos manuales) de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.

d) Seleccionar contraseñas de calidad con longitud mínima suficiente que:

   1) Sean fáciles de recordar.

   2) No se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.

   3) No sean vulnerables al ataque de diccionarios (es decir, que no consistan en palabras incluidas en diccionarios).

   4) No tengan caracteres idénticos consecutivos, que no sean todos numéricos ni todos alfabéticos.

e) Cambiar las contraseñas a intervalos regulares o con base en el número de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas.

f) Cambiar las contraseñas temporales en el primer registro de inicio.

g) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.

h) No compartir las contraseñas de usuario individuales.

i) no utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que pueden usar una sola contraseña de calidad para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

11.3.2 Equipo de usuario desatendido

Control

Los usuarios deberían asegurarse de que los equipos desatendidos tengan protección apropiada.

Guía de implementación

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) Terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña.

b) Realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal).

c) Cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña.

11.3.3 Política de escritorio despejado y de pantalla despejada

Control

Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

Guía de implementación

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) Cuando no se requiere la información sensible o crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave (idealmente una caja fuerte, un gabinete u otro mueble de seguridad), especialmente cuando la oficina está vacía.

b) Las sesiones de los computadores y los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un *token* o un mecanismo similar de autenticación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando.

c) Se deberían proteger los puntos de entrada y salida de correo y las máquinas de facsímil desatendidas.

d) Es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, etc.).

e) Los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.

11.7.1 Computación y comunicaciones móviles

Control

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Guía de implementación

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (*notebooks*), microcomputadores de bolsillo (*palmtops*), y computadores portátiles pesados (*laptops*), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos sin protección.

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio. Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información. Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes debería tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y / o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

11.7.2 Trabajo remoto

Control

Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guía de implementación

Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo, robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.

b) El entorno físico de trabajo remoto propuesto.

c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno.

d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos.

e) El uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.

f) Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.

g) El acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley.

h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

i) Protección antivirus y requisitos de barreras contra fuego (firewall).

Las directrices y disposiciones a considerar deberían incluir las siguientes:

a) Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.

b) Definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.

c) Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.

d) Seguridad física.

e) Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

f) Disposición de soporte y mantenimiento de hardware y software.

g) Disposición de pólizas de seguros.

h) Procedimientos para el respaldo y la continuidad del negocio.

12.3.1 Política sobre el uso de controles criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Guía de implementación

Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

a) El enfoque de la dirección hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.

b) Con base en la evaluación de riesgos, se debería identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.

c) Uso de encriptación para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos o a través de las líneas de comunicación.

d) Enfoque para la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.

e) Funciones y responsabilidades, por ejemplo, quién es responsable de:

   1) La implementación de la política.

   2) La gestión de claves, incluyendo su generación.

f) Normas que se han de adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio).

g) Impacto de la utilización de información encriptada sobre los controles que depende dela inspección del contenido (por ejemplo, detección de virus).

Cuando se implementa la política de encriptación de la organización, es conveniente tener en mente los reglamentos y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los aspectos del flujo trans-fronterizo de información encriptada.

Los controles criptográficos se pueden utilizar para lograr diferentes objetivos de seguridad, por

ejemplo:

a) Confidencialidad: uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.

b) Integridad / autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.

c) No-repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implementación

Se deberían tomar en consideración las siguientes directrices para proteger todo el material que se pueda considerar propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.

b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

c) Mantener la concientización de sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que lo viole.

d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

f) Implementar controles para asegurar que no se excede al número máximo de usuarios permitidos.

g) Verificar que únicamente se instalan software autorizado y productos con licencias.

h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar las herramientas de auditoría adecuada.

k) Cumplir los términos y condiciones para el software y la información obtenido de redes públicas.

l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.

m) No copiar total ni parcialmente libros, archivos, informe ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información

Control

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

Guía de implementación

La dirección debería aprobar el uso de los servicios de procesamiento de información. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecutó.

Se deberían registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

Pregunte y confirmar si existe un oficial del riesgo de TI y de control, esto sobre la base de estándares reconocido en la industria normas / dirección y prácticas más importantes (por ejemplo, COSO, COSO-ERM, COBIT).

Evaluar si el riesgo de TI y marco de control está alineado con el riesgo empresarial de la organización y marco de control y considera que el riesgo empresarial nivel de tolerancia. Pregunte y confirme si el riesgo de TI y marco de control especifica su alcance y finalidad y se proyectan las expectativas de la dirección de lo que debe ser controlado.

Pregunte y confirme si la estructura de los riesgos de TI y de control está bien definida y responsabilidades han sido claramente establecidos y asignados a las personas apropiadas.

Pregunte y confirme si un proceso está en su lugar que revise periódicamente (preferiblemente cada año) los riesgos de TI y el marco de control para mantener su adecuación y la relevancia.

PO6.3 Administración de Políticas para TI

Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización, incluyendo los siguientes:

    1) Cumplimiento de los requisitos legales, reglamentarios y contractuales.

    2) Requisitos de educación, formación y concientización sobre seguridad.

    3) Gestión de la continuidad del negocio.

    4) Consecuencias de las violaciones de la política de seguridad.

e) Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

Guías de Aseguramiento

- Pregunte y confirme si un conjunto jerárquico de las políticas, normas y procedimientos se han creado y adaptado a la estrategia de TI y el medio ambiente del control.
- Pregunte y confirme si las políticas específicas pertinentes existen en temas clave, tales como la calidad, seguridad, confidencialidad, controles internos, la ética y los derechos de propiedad intelectual.
- Pregunte y confirme si se ha definido un proceso de actualización de la política que requiere, como mínimo, los exámenes anuales.
- Pregunte y confirme que se establezcan procedimientos para realizar seguimiento de cumplimiento y definir las consecuencias de su incumplimiento.
- Pregunte y confirme si la rendición de cuentas que se ha definido y documentado para formular, desarrollar, documentar, ratificar, difundir y controlarlas políticas para asegurar que todos los elementos del proceso de gestión de la política han sido asignados a los individuos responsables.

PO6.4 Implantación de Políticas de TI

Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

   4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente. Que tienen que ver con el siguiente ítem.

7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

3) Proceso de autorización para los privilegios y el acceso de usuario.

4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

   1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

   2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

   3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Pregunte y confirme si hay un proceso en marcha para transcribir las políticas y normas en los procedimientos operativos.
- Pregunte y confirme si los contratos de trabajo y mecanismos de incentivos están alineados con las políticas.
- Pregunte y confirme si hay un proceso en marcha para exigir a los usuarios que reconozcan explícitamente que han recibido, comprendido y aceptado las políticas de TI, las normas y los procedimientos pertinentes. El acuse de recibo se actualiza periódicamente (por ejemplo, cada dos años).
- Pregunte si los recursos son suficientes y calificados están disponibles para apoyar el despliegue de políticas.

PO6.5 Comunicación de los Objetivos y la Dirección de TI

Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

   Incluyendo los siguientes:

   1) Cumplimiento de los requisitos legales, reglamentarios y contractuales.

   2) Requisitos de educación, formación y concientización sobre seguridad.

   3) Gestión de la continuidad del negocio.

   4) Consecuencias de las violaciones de la política de seguridad.

e) Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información.

f) Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

La dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

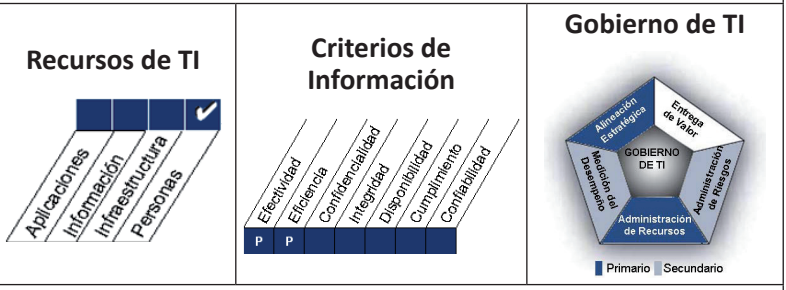
Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

Guías de Aseguramiento

- Pregunte y confirme si hay procesos de gestión para comunicar los objetivos de TI con regularidad y dirección.
- Verifique con una muestra representativa de los funcionarios de distintos niveles que lo objetivos han sido claramente comunicados y comprendidos.
- Revisar comunicaciones pasadas y verificar que cubre la misión, los objetivos de servicio, seguridad, controles internos, la calidad, código de ética y conducta, políticas y procedimientos, etc.

P07. Administrar los Recursos Humanos de TI.

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.



PO7.1 Reclutamiento y Retención del Personal

Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (Ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.1.2 Selección

Control

Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Guías de implementación

En las revisiones de verificación se deberían tener en cuenta la legislación pertinente a la privacidad, la protección de datos personales y / o el empleo y cuando se permite, debería incluir lo siguiente:

a) Disponibilidad de referencia de comportamiento satisfactorio, por ejemplo una laboral y otra personal.

b) Una verificación (para determinar la totalidad y exactitud) de la hoja de vida del candidato.

c) Confirmación de las calificaciones profesionales y académicas declaradas.

d) Verificación de la identidad independiente (pasaporte o documento similar).

e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible, como por ejemplo información financiera o de alta confidencialidad, la organización debería considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y las limitaciones para las revisiones de verificación, por ejemplo quien es elegible para seleccionar al personal y cómo, cuándo y por qué se realizan las verificaciones.

También deberían llevar a cabo un proceso de selección para los contratistas y los usuarios de terceras partes. Cuando los contratistas son suministrados por una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para la selección y los procedimientos de notificación que es necesario seguir si la selección no se ha completado o si los resultados arrojan dudas o preocupación. De la misma manera, el acuerdo de la tercera parte debería especificar claramente todas las responsabilidades y los procedimientos de la notificación para la selección.

Informar sobre todos los candidatos que se consideran para los cargos dentro de la organización se debería recolectar y manejar según la legislación adecuada existente en la jurisdicción correspondiente.

Dependiendo de la legislación que se aplique, se debería informar con anticipación a los candidatos sobre las actividades de selección.

8.1.3 Términos y condiciones laborales

Control

Como parte de la obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

Guías de implementación

Los términos y condiciones laborales deberían refleja la política de seguridad de la organización, además debería aclarar y establecer:

a) Que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a la información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información.

b) Los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o legislación sobre protección de datos.

c) Responsabilidades para la clasificación de la información y la gestión de los activos asociados con sistemas y servicios de información manejados por el empleado, el contratista o usuario de tercera parte.

d) Responsabilidades del empleado, contratista o usuario de tercera parte para el manejo de información recibida de otras empresas o de partes externas.

e) Responsabilidades de la organización para el manejo de la información personal, incluyendo la información personal creada como resultado o durante el contrato laboral con la organización.

f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio.

g) Acciones a tomar si el empleado, contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

La organización debería garantizar que los empleados, los contratistas y los usuarios de terceras partes están de acuerdo con los términos y condiciones respecto a la seguridad de la información según la naturaleza del acceso que tendrán a los activos de la organización asociado con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones laborales deberían durante un período definido después de la terminación del contrato laboral.

Guías de Aseguramiento

- Pregunte y confirme si existe un plan de gestión de recursos humanos de TI, que refleja la definición de requisitos de formación y cualificación profesional elegida para satisfacer táctica y estratégicamente TI de la organización. El plan debe ser actualizado al menos una vez al año y debe incluir medidas específicas de contratación y retención de los planes frente a las necesidades actuales y futuras. También debe incluir políticas para la aplicación de los procedimientos de interrupción de vacaciones, según corresponda.

- Pregunte y confirme si hay un proceso documentado para la contratación y retención de personal de TI está en su lugar y refleja las necesidades identificadas en el plan de recursos humanos de TI.

- Confirme que los profesionales de RR.HH. periódicamente revisan y aprueban el proceso de reclutamiento y de TI de retención para asegurar la alineación con las políticas de la organización.

PO7.2 Competencias del Personal

Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Inspeccionar una muestra de las descripciones de los puestos para una descripción completa y apropiada de las habilidades necesarias, las competencias y cualificaciones.
- Verificar que los procesos existen y se llevan a cabo de forma periódica para revisar y actualizar las descripciones de puestos.
- Pregunte y confirme si, la dirección ha identificado las necesidades de cualificación, incluida la educación apropiada, entrenamiento cruzado y requisitos de certificación a la dirección de los requisitos específicos de la organización.

PO7.3 Asignación de Roles

Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.1.3 Términos y condiciones laborales

Control

Como parte de la obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual deber establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

Guías de implementación

Los términos y condiciones laborales deberían refleja la política de seguridad de la organización, además debería aclarar y establecer:

a) Que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a la información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información.

b) Los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o legislación sobre protección de datos.

c) Responsabilidades para la clasificación de la información y la gestión de los activos asociados con sistemas y servicios de información manejados por el empleado, el contratista o usuario de tercera parte.

d) Responsabilidades del empleado, contratista o usuario de tercera parte para el manejo de información recibida de otras empresas o de partes externas.

e) Responsabilidades de la organización para el manejo de la información personal, incluyendo la información personal creada como resultado o durante el contrato laboral con la organización.

f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio.

g) Acciones a tomar si el empleado, contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

La organización debería garantizar que los empleados, los contratistas y los usuarios de terceras partes están de acuerdo con los términos y condiciones respecto a la seguridad de la información según la naturaleza del acceso que tendrán a los activos de la organización asociado con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones laborales deberían durante un periodo definido después de la terminación del contrato laboral.

8.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, contratistas y los usuarios de terceras partes:

a) Están adecuadamente informados sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se le otorgue acceso a la información o sistemas de información sensible.

b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.

c) Estén motivados para cumplir las políticas de seguridad de la organización.

d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización, teniendo en cuenta el siguiente ítem.

e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen las políticas de seguridad de la información de la organización y los métodos apropiados de trabajo.

f) Sigan teniendo las calificaciones y habilidades apropiadas.

Guías de Aseguramiento

- Inspeccionar una muestra de descripciones de funciones para asegurar la inclusión de una definición adecuada de las responsabilidades, competencias y sensible de la seguridad y los requisitos de cumplimiento.

- Inspeccionar una muestra de reconocimiento a la aceptación de las descripciones de funciones y responsabilidades para el personal de TI.
- Revisar los términos y condiciones de empleo por la existencia de no-divulgación, los derechos de propiedad intelectual, la responsabilidad de seguridad de la información, control interno, las leyes aplicables y los requisitos. Estos deben estar alineados con los requisitos de la organización para la no-divulgación de información confidencial.
- Inspeccione la muestra de descripciones de trabajo para puestos de alto riesgo para determinar si el alcance del control y si es necesario un control adecuado para cada función.

PO7.4 Entrenamiento del Personal de TI

Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Camine por el proceso de capacitación para confirmar que la formación crítica y los requisitos del conocimiento están incluidos.
- Inspeccione el contenido de los programas de formación para la integridad y la idoneidad.
- Inspeccione los mecanismos de entrega de los recursos de TI para determinar si la información se entrega a todos los usuarios, incluidos los consultores, contratistas, agentes temporales y, en su caso, los clientes y proveedores.
- Inspeccione el contenido del programa de capacitación para determinar si todos los marcos de control interno y los requisitos de seguridad se incluyen sobre la base de las políticas de seguridad de la organización y los controles internos (por ejemplo, el impacto de la no-adhesión a los requisitos de seguridad, uso adecuado de los recursos de la empresa y las instalaciones, manejo de incidentes, de los empleados responsabilidad de la seguridad de la información).
- Pregunte y confirme si los materiales y programas de formación han sido revisados regularmente para su adecuación.

- Revise la política para determinar las necesidades de formación. Confirme que la política de los requisitos de formación garantiza que los requisitos críticos de la organización se reflejan en programas de formación y sensibilización.

PO7.6 Procedimientos de Investigación del Personal

Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

8.1.2 Selección

Control

Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Guías de implementación

En las revisiones de verificación se deberían tener en cuenta la legislación pertinente a la privacidad, la protección de datos personales y / o el empleo y cuando se permite, debería incluir lo siguiente:

a) Disponibilidad de referencia de comportamiento satisfactorio, por ejemplo una laboral y otra personal.

b) Una verificación (para determinar la totalidad y exactitud) de la hoja de vida del candidato.

c) Confirmación de las calificaciones profesionales y académicas declaradas.

d) Verificación de la identidad independiente (pasaporte o documento similar)

e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible, como por ejemplo información financiera o de alta confidencialidad, la organización debería considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y las limitaciones para las revisiones de verificación, por ejemplo quien es elegible para seleccionar al personal y cómo, cuándo y por qué se realizan las verificaciones.

También deberían llevar a cabo un proceso de selección para los contratistas y los usuarios de terceras partes. Cuando los contratistas son suministrados por una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para la selección y los procedimientos de notificación que es necesario seguir si la selección no se ha completado o si los resultados arrojan dudas o preocupación. De la misma manera, el acuerdo de la tercera parte debería especificar claramente todas las responsabilidades y los procedimientos de la notificación para la selección.

Informar sobre todos los candidatos que se consideran para los cargos dentro de la organización se debería recolectar y manejar según la legislación adecuada existente en la jurisdicción correspondiente.

Dependiendo de la legislación que se aplique, se debería informar con anticipación a los candidatos sobre las actividades de selección.

Guías de Aseguramiento

- Inspeccione los criterios de selección para la ejecución de los controles de seguridad de fondo de liquidación.
- Revisión de la definición adecuada de funciones críticas, para lo cual los controles de autorización de seguridad se requieren. Esto debería aplicarse a los empleados, contratistas y proveedores.
- Averiguar y confirmar si los procesos de contratación incluyen control a fondo. Inspeccionar la documentación para contratar una muestra representativa de los miembros del personal de TI a evaluar si la revisión de antecedentes se ha completado y evaluado.

PO7.7 Evaluación del Desempeño del Empleado

Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Inspeccionar una muestra representativa de las evaluaciones de desempeño de los empleados de trabajo para determinar si los criterios para el establecimiento de metas incluye objetivos SMARRT. Éstos deben reflejan las competencias básicas, valores de la compañía y habilidades necesarias para cada función. A través del proceso de trabajo de evaluación del desempeño para determinar si las políticas y procedimientos para el uso y almacenamiento de información personal son claras y cumplir con la legislación aplicable.

- Inspeccione la remuneración / reconocimiento de proceso para determinar si está en conformidad con los objetivos de rendimiento y la política de la organización.

- Inspeccione los planes de mejora del rendimiento para determinar la alineación con las políticas de organización y la aplicación coherente en toda la organización de TI. Los planes de mejora deben incluir metas específicamente definidas, plazos de ejecución y un nivel adecuado de medidas disciplinarias si no se logran mejoras.

PO7.8 Cambios y Terminación de Trabajo

Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

8.2.3 Proceso disciplinario

Control

Debería existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.

Guía de implementación

No se recomienda iniciar el proceso disciplinario antes de verificar que se ha presentado la violación de la seguridad.

El proceso disciplinario formal debería garantizar el tratamiento imparcial y correcto para los empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal debería brindar una respuesta gradual que considere factores tales como la naturaleza y la gravedad de la violación y su impacto en el negocio, si es la primera ofensa o se repite, si el violador está capacitado adecuadamente, la legislación correspondiente, los contratos de negocio y otros factores, según el caso. En los casos graves de mala conducta el proceso debería permitir el retiro instantáneo de las funciones, los derechos de acceso y los privilegios y el acompañamiento inmediato fuera de las instalaciones, si es necesario.

8.3.1 Responsabilidades en la terminación

Control

Se deberían definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.

Guía de implementación

La comunicación de las responsabilidades en la terminación debería incluir los requisitos permanentes de seguridad y las responsabilidades legales y, cuando sea apropiado, las responsabilidades contenidas en cualquier acuerdo de confidencialidad y los términos y condiciones laborales deberían continuar durante un periodo definido después de terminar la contratación laboral del empleado, el contratista o el usuario de terceras partes.

Los contratos del empleado, el contratista o el usuario de terceras partes deberían incluir las responsabilidades y deberes válidos aún después de la terminación del contrato laboral.

Los cambios en la responsabilidad o en el contrato laboral deberían ser gestionados como la terminación de la responsabilidad o el contrato laboral respectivo, y la nueva responsabilidad o contrato laboral se debería controlar tal como se describe en el numeral 8.1.

8.3.2 Devolución de activos

Control

Todos los empleados, contratistas o usuarios de terceras partes deberían devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.

Guía de implementación

Se debería formalizar el proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la organización tales como los dispositivos de cómputo móviles, las tarjetas de crédito, las tarjetas de acceso, el software, los manuales y la información almacenada en medios electrónicos.

Cuando un empleado, contratista o usuario de terceras partes adquiere equipo de la organización o utiliza su propio equipo, se deberían seguir los procedimientos para garantizar que toda la información pertinente se transfiere a la organización y se elimina con seguridad de tal equipo.

Cuando un empleado, contratista o usuario de terceras partes tiene un conocimiento que es importante para la continuación de las operaciones, esa información debería estar documentada y transferirse a la organización.

8.3.3 Retiro de los derechos de acceso

Control

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deberían retirar al finalizar su contratación laboral, contrato o acuerdo o se deberían ajustar después del cambio.

Guía de implementación

Después de la terminación, se deberían reconsiderar los derechos de acceso de la persona a los activos asociados con los sistemas y servicios de información. Ello determinará si es necesario retirar los derechos de acceso. Los cambios en un cargo se deberían reflejar en el retiro de todos los derechos de acceso que no estén aprobados para el nuevo cargo. Los derechos de acceso que se deberían adaptar o retirar incluyen acceso físico y lógico, claves, tarjetas de identificación, servicios de procesamiento de información, suscripciones y retiro de cualquier documentación que lo identifique como miembro actual de la organización. Si un empleado, contratista o usuario de terceras partes que se retira tiene contraseñas conocidas para permanecer activo, éstas se deberían cambiar en la terminación o el cambio de empleo, contrato o acuerdo.

Los derechos de acceso a los activos de información y a los servicios de procesamiento de información se deberían reducir o retirar antes de la finalización o cambio del contrato laboral, dependiendo de la evaluación de factores de riesgo tales como:

a) Si la terminación o el cambio es iniciativa del empleado, contratista o usuario de terceras partes o por la dirección y el motivo de dicha terminación.

b) Las responsabilidades actuales del empleado, contratista o cualquier otro usuario.

c) El valor de los activos actualmente accesibles.

Guías de Aseguramiento

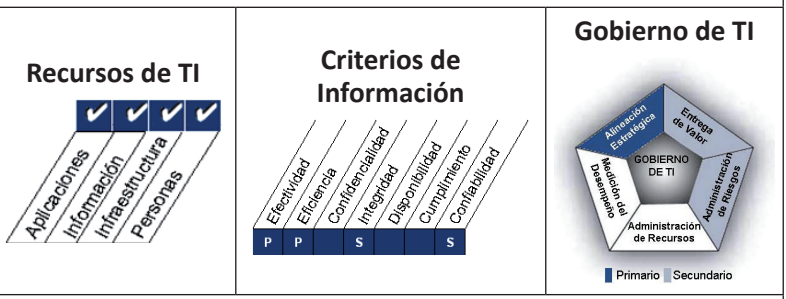
- Pregunte y compruebe si los procedimientos de salida para la interrupción voluntaria del empleo están documentados y contienen todos los elementos necesarios, tales como el conocimiento necesario de transferencia, a tiempo de asegurar el acceso físico y lógico, el rendimiento de los activos de la organización y realización de entrevistas de salida.

- Averiguar si los procedimientos de cambio de empleo están documentados y contienen todos los elementos necesarios para minimizar la interrupción de los procesos de negocio. Los ejemplos incluyen la necesidad de orientación laboral, trabajo a mano sobre los pasos y la formación formal de preparación. Inspeccione los procedimientos de cambio de trabajo para determinar si los procedimientos son seguidos consistentemente.

- Adquirir recursos humanos a través de una lista de terminado / transferir a usuarios (durante los últimos seis meses a un año).

P08. Administrar la Calidad.

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.



PO8.3 Estándares de Desarrollo y de Adquisición

Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida hasta el último entregable, e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como “necesidad de conocer”).

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

    1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

    2) Todos y los controles y mecanismos de protección física requeridos.

    3) Controles para asegurar la protección contra software malicioso.

    4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

    5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

    6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

    7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

   1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

   2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

   3) Proceso de autorización para los privilegios y el acceso de usuario.

   4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

   5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

   6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad (7.2.1).

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países (15.1).

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias (15.1.2) y la protección de cualquier trabajo en colaboración (6.1.5).

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

12.5.5 Desarrollo de software contratado externamente

Control

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

Guía de implementación

Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

a) Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.

b) Certificación de la calidad y exactitud del trabajo realizado.

c) Convenios de fideicomiso en caso de falla de la tercera parte.

d) Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.

e) Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.

f) Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

Guías de Aseguramiento

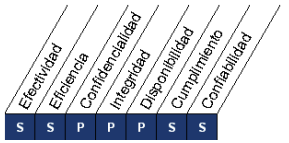
- Averiguar si el desarrollo y la adquisición de normas para los cambios de TI de los recursos existentes se aplican (por ejemplo, prácticas de codificación segura, normas de codificación de software, convenciones de nombres, formatos de archivo; esquema y diccionario de datos estándares de diseño, normas de interfaz de usuario, la interoperabilidad, la eficiencia de rendimiento del sistema, escalabilidad , las normas para el desarrollo y pruebas, validación respecto a los requisitos, planes de prueba, unidad, la regresión y la prueba de integración).

- Averiguar o inspeccionar si las normas de desarrollo y adquisición de permitir un nivel adecuado de control de cambios en los recursos de TI.

- Averiguar si el desarrollo y orientación de adquisición se incorpora a estándares de TI y los marcos.

P09. Evaluar y Administrar los Riesgos de TI.

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

Recursos de TI	Criterios de Información	Gobierno de TI
		

PO9.1 Marco de Trabajo de Administración de Riesgos

Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar unaestrategia de continuidad del negocio para determinar el enfoque global para la continuidad delnegocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se deberíacrear y respaldar un plan para la implementación de esta estrategia.

Guías de Aseguramiento

- Inspeccione si los riesgos de TI se alinean al marco de gestión con el marco de la gestión de riesgos para la organización (empresa) e incluye negocios impulsados por componentes de la estrategia, programas, proyectos y operaciones. Revise las clasificaciones de riesgos de TI, para comprobar que se basan en un conjunto común de características del marco de gestión riesgo empresarial. Inspeccione si las mediciones de riesgo están estandarizadas y priorizadas y si incluyen el impacto, la aceptación del riesgo residual y las probabilidades en consonancia con el marco de la empresa de gestión de riesgos.
- Compruebe si los riesgos de TI son considerados en la elaboración y revisión de planes estratégicos de TI.

PO9.2 Establecimiento del Contexto del Riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

Guías de Aseguramiento

- Pregunte y confirme si se ha definido un contexto de riesgo adecuada de acuerdo con las políticas de gestión del riesgo empresarial y los principios e incluye los procesos, tales como los sistemas, gestión de proyectos, ciclos de vida del software de aplicación, la gestión de las operaciones de TI y servicios. Factores internos y externos de riesgo deben ser incluidos.

- Determinar si los riesgos de TI del contexto es comunicada y entendida.

PO9.3 Identificación de Eventos

Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

13.1.1 Reporte sobre los eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Guía de implementación

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empelados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema.

b) Formatos para el reporte de los eventos de seguridad de la información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información.

c) El comportamiento correcto en caso de un evento de seguridad de la información, es decir:

    1) Tomar nota inmediatamente sobre los detalles importantes (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño).

    2) No ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto.

d) Referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de la seguridad.

En entornos de alto riesgo, se puede suministrar una alarma de coacción4) a través de la cual una persona bajo coacción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coacción deberían reflejar la situación de alto riesgo que indican tales alarmas.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

Guías de Aseguramiento

- Inspeccione el proceso utilizado para identificar eventos potenciales y determinar si todos los procesos de TI se incluyen en el análisis. El diseño del proceso deberían cubrir los eventos internos y externos. Identificación de posibles eventos pueden incluir los resultados de las auditorías anteriores, las inspecciones e incidentes identificados, utilizando listas de control, talleres y análisis de flujo de proceso. Trace los impactos identificados en el registro de riesgos para determinar si el registro es completo, actualizado y en línea con el marco de la empresa de gestión de riesgos de terminología.

- Averiguar si adecuados equipos multi-funcionales están involucrados en el evento y actividades de diferentes efectos de identificación. Revisión de una muestra del registro de riesgo de importancia de las amenazas, la importancia de las vulnerabilidades y la importancia del impacto, y analizar la eficacia del proceso para identificar, registrar y los riesgos conocidos.

PO9.4 Evaluación de Riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

d) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

e) Mejora de los objetivos de control y de los controles.

f) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

Guías de Aseguramiento

- Camine por el proceso de gestión de riesgos para determinar si los riesgos inherentes y residuales son definidos y documentados.

- Averiguar y confirmar si el proceso de gestión de riesgos evalúa los riesgos identificados cualitativa y/o cuantitativamente.

- Inspeccione el proyecto y demás documentación para evaluar la idoneidad de la evaluación de riesgos cualitativa o cuantitativa.

- Camine a través del proceso para determinar si las fuentes de información utilizadas en el análisis son razonables.

- Inspeccionar el uso de análisis estadísticos y las determinaciones de probabilidad para medir la probabilidad cualitativa o cuantitativamente.

- Averiguar o inspeccionar si existe alguna correlación entre los riesgos que se identifica. Revise cualquier correlación para verificar que expone significativamente diferente probabilidad y los resultados de impacto derivados de dicha relación (s).

APÉNDICE B

GUÍAS PARA EL DOMINIO DE ADQUIRIR E IMPLEMENTAR

ADQUIRIR E IMPLEMENTAR (AI)

AI1 Identificar Soluciones Automatizadas

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de "desarrollar" o "comprar". Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.

Recurso de TI	Criterios de Información	Gobierno de TI
		

AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio

Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Guía de implementación

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

Guías de Aseguramiento

- Confirmar a través de entrevistas con miembros clave del personal si las necesidades funcionales y técnicos del negocio han sido definidos y si un proceso de mantenimiento se ha acordado. Revise la documentación de requisitos y procesos de mantenimiento, y asegúrese que el diseño es apropiado para el tamaño, la complejidad, los objetivos y los riesgos de la adquisición y que ha sido aprobado por el correspondiente propietario / patrocinador.
- Confirmar a través de entrevistas con miembros clave del personal que todos los requisitos y criterios de aceptación relevantes han sido considerados, capturado, priorizados y registrados de una manera que sea comprensible para los interesados y patrocinadores.
- Confirmar a través de entrevistas con miembros clave del personal que los requisitos de aplicaciones y la infraestructura técnica satisface las necesidades de las normas de la organización para la arquitectura de la información y la dirección técnica estratégica.
- Revisar los planes, políticas y procedimientos para identificar excepciones o desviaciones de los estándares de arquitectura de la información y la dirección técnica estratégica.

AI1.2 Reporte de Análisis de Riesgos

Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación.

b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Guía de implementación

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Guías de Aseguramiento

- Confirmar a través de entrevistas con funcionarios clave, la inspección de la documentación del proyecto, etc., que se usa una aproximación holística para el análisis de riesgos de la las nuevas solución automatizada.
- Confirmar a través de entrevistas que las partes interesadas están involucradas en el proceso, incluyendo representantes de negocios y de TI.
- Pregunte y confirme si, los mecanismos apropiados de mitigación de riesgo son considerados en el diseño y contribución de la solución desde la metodología, si son justificados por los riesgos que enfrenta la organización.

AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación

Verificar que el proceso requiere al patrocinador del negocio para aprobar y autoriza los requisitos de negocio, tanto funcionales como técnicos, y los reportes del estudio de factibilidad en las etapas clave predeterminadas. El patrocinador del negocio tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

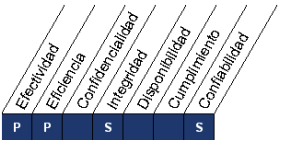
Guías de Aseguramiento

- Confirmar a través de entrevistas con el patrocinador de negocios que los controles de calidad y los reportes de factilidad se llevan a cabo para los requisitos funcionales y técnicos y que el patrocinador de negocios es consciente de los criterios originales de aceptación.

- Evaluar la documentación de proyectos para una muestra representativa de los proyectos para asegurarse de que el patrocinadordel negocio ha aprobado los requerimientos funcionales y técnicospara los informes de factibilidad.

AI2 Adquirir y Mantener Software Aplicativo

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.

Recurso de TI	Criterios de Información	Gobierno de TI
		

AI2.3 Control y Posibilidad de Auditar las Aplicaciones

Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.

10.10.1 Registro de auditorías

Control

Se deberían elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.

Guía de implementación

Los registros para auditoría deberían incluir, cuando corresponda.

a) identificación (ID) de usuario.

b) fecha, hora y detalles de los eventos clave, por ejemplo registro de inicio y registro de cierre.

c) identidad o ubicación de la terminal, si es posible.

d) registros de los intentos aceptados y rechazados de acceso al sistema.

e) registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.

f) cambios en la configuración del sistema.

g) uso de privilegios.

h) uso de las utilidades y aplicaciones del sistema.

i) archivos a los que se ha tenido acceso y tipo de acceso.

j) direcciones y protocolos de red.

k) alarmas originadas por el sistema de control del acceso.

l) activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

10.10.5 Registro de fallas

Control

Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas.

Guía de implementación

Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistemarelacionadas con problemas de procesamiento de la información o con los sistemas decomunicación. Deberían existir reglas claras para el manejo de las fallas reportadas,incluyendo:

a) revisión de los registros de fallas para garantizar que las éstas se han resuelto satisfactoriamente.

b) revisión de las medidas correctivas para garantizar que no se han puesto en peligro loscontroles y que la acción tomada está totalmente autorizada.

Se debería asegurar que el registro de errores está habilitado, si esta función del sistema estádisponible.

12.2.1 Validación de los datos de entrada

Control

Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

Guía de implementación

Es recomendable realizar verificaciones de las entradas de las transacciones del negocio, de los datos permanentes (por ejemplo, nombres y direcciones, límites de crédito, números de referencia del cliente) y de las tablas de parámetros (por ejemplo, precios de venta, tasas de conversión de divisas, tasas de impuestos). Se recomienda tomar en consideración las siguientes directrices:

a) verificaciones de entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar los siguientes errores:

   1) valores fuera de rango.

   2) caracteres no válidos en los campos de datos.

   3) datos incompletos o ausentes.

   4) exceso en los límites superiores e inferiores del volumen de datos.

   5) datos de controles inconsistentes o no autorizados.

b) revisión periódica del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.

c) inspección de los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).

d) procedimientos de respuesta ante errores de validación.

e) procedimientos para probar la credibilidad de los datos de entrada.

f) definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.

g) creación de un registro de las actividades implicadas en el proceso de entrada de datos.

12.2.2 Control de procesamiento interno

Control

Se deberían incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.

Guía de implementación

El diseño y la implementación de las aplicaciones deberían garantizar que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

a) utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos.

b) procedimientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de falla previa del procesamiento.

c) utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos.

d) protección contra ataques empleando desbordamiento / exceso en el búfer.

Se deberían elaborar listas de verificación adecuadas, documentar las actividades y mantener seguros los resultados. Los siguientes son algunos ejemplos de verificaciones que se pueden incorporar:

a) controles de sesión o de lotes, para conciliar los balances de archivos de datos después de actualizar las transacciones.

b) controles de balance, para verificar los balances de apertura frente a los balances decierre previos, a saber:

   1) controles para cada ejecución.

   2) totales de actualizaciones de archivos.

   3) controles programa a programa.

c) validación de los datos de entrada generados por el sistema.

d) verificaciones de la integridad, la autenticidad o cualquier otra característica deseguridad de los datos o del software descargado o actualizado entre el computadorcentral y el remoto.

e) totales de verificación (*hash*) de registros y archivos.

f) verificaciones para garantizar que los programas de aplicación se ejecutan en el momento correcto.

g) verificaciones para garantizar que los programas se ejecutan en el orden correcto yterminan en caso de falla, y que el procesamiento posterior se detiene hasta resolver el problema.

h) creación de un registro de las actividades implicadas en el procesamiento.

12.2.3 Integridad del mensaje

Control

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

Guía de implementación

Se debería realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

12.2.4 Validación de los datos de salida

Control

Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

Guía de implementación

La validación de los datos de salida puede incluir:

a) verificaciones de la verosimilitud para probar si los datos de salida son razonables.

b) cuentas de control de conciliación para asegurar el procesamiento de todos los datos.

c) suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información.

d) procedimientos para responder las pruebas de validación de salidas.

e) definición de las responsabilidades de todo el personal que participa en el proceso de la salida de datos.

f) creación de un registro de las actividades del proceso de validación de la salida de datos.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

15.3.1 Controles de auditoría de los sistemas de información

Control

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

Guía de implementación

Se deberían tener presente las siguientes directrices:

a) los requisitos de auditoría se deberían acordar con la dirección correspondiente.

b) se debería acordar y controlar el alcance de las verificaciones.

c) las verificaciones se deberían limitar al acceso de sólo lectura del software y los datos.

d) el acceso diferente al de sólo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.

e) los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles.

f) se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.

g) todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar para datos o sistemas críticos.

h) se recomienda documentar todos los procedimientos, requisitos y responsabilidades.

i) la persona que realiza la auditoría debería ser independiente de las actividades auditadas.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

Guía de implementación

Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativos y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

Guías de Aseguramiento

- Revisar la documentación de los requisitos para el diseño de controles para determinar que los controles automatizados de aplicación están definidosbasados en requisitos de control de procesos de negocio.
- Revisar la documentación de requisitos para el diseño de controles, e identifique los casos donde son inadecuados los controles de autorización, de entrada, procesamiento, de salida y de límite de datos.
- Revisar los planes para implementar funciones de control automatizada en paquetes de software, y determine que los requisitos de control de procesos de negocios están trazados adecuadamente.
- Confirmar con los dueños de procesos de negocio y las autoridades técnicas de diseño que las especificaciones de diseño para todos los controles automatizados de la aplicación en desarrollo o adquisiciones son aprobadas.
- Revise las especificaciones del diseño para todos los controles automatizados de la aplicación en desarrollados o adquiridos / empaquetadas para confirmar que son aprobados.
- Confirme con el personal de proyectos que los controles automatizados se han definido dentro de la aplicación y que apoyan los objetivos de control generales, tales como la seguridad, integridad de datos, rastros de auditoría, control de accesos y controles de integridad de base de datos.
- Realizar revisiones de los controles de aplicación de software desarrollados o adquirido envasados, siga y revise las transacciones, y la documentación para garantizar que los objetivos de control generales (por ejemplo, la seguridad, integridad de datos, rastros de auditoría, control de acceso, controles de integridad de base de datos) sean atendidos adecuadamente.

- Examen la documentación del proyecto para confirmar que las especificaciones de diseño han sido determinadoscontra la auditoría interna, control y estándares y objetivos de la gestión del riesgo.

- Repase la documentación del proyecto para determinar si los efectos de los controles compensatorios fuera del entorno de aplicación de software han sido considerados.

- Revisión de pruebas de alto nivel para asegurarse que los controles automatizados y los objetivos generales de control son alcanzados (por ejemplo, disponibilidad, seguridad, exactitud, exhaustividad, actualidad, la autorización, la auditabilidad).

AI2.4 Seguridad y Disponibilidad de las Aplicaciones

Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

7.2.1 Directrices de clasificación

Control

La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

Guía de implementación

Las clasificaciones y los controles de protección deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

Las directrices de clasificación deberían incluir convecciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con una política predeterminada de control del acceso.

Debería ser responsabilidad del propietario del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado. La clasificación debería considerar el efecto de suma mencionado en el numeral 10.7.2.

Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación.

b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Guía de implementación

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

12.2.3 Integridad del mensaje

Control

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

Guía de implementación

Se debería realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

12.3.1 Política sobre el uso de controles criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Guía de implementación

Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

a) el enfoque de la dirección hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.

b) con base en la evaluación de riesgos, se debería identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.

c) uso de encriptación para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos o a través de las líneas de comunicación.

d) enfoque para la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.

e) funciones y responsabilidades, por ejemplo, quién es responsable de:

   1) la implementación de la política;

   2) la gestión de claves, incluyendo su generación.

f) normas que se han de adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio).

g) impacto de la utilización de información encriptada sobre los controles que depende de la inspección del contenido (por ejemplo, detección de virus).

Cuando se implementa la política de encriptación de la organización, es conveniente tener en mente los reglamentos y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los aspectos del flujo trans-fronterizo de información encriptada.

Los controles criptográficos se pueden utilizar para lograr diferentes objetivos de seguridad, por

ejemplo:

a) confidencialidad: uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.

b) integridad / autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.

no-repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

12.4.3 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implementación

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas, con el objeto de reducir el potencial de corrupción de los programas de computador:

a) cuando sea posible, las librerías fuente de programas no se deberían mantener en lossistemas operativos.

b) el código fuente de programas y las librerías fuente de programas se deberían gestionarde acuerdo con los procedimientos establecidos.

c) el personal de soporte debería tener acceso restringido a las librerías fuente de programas.

d) la actualización de las librerías fuente de programas y de los elementos asociados, asícomo la emisión de fuentes de programa a los programadores, solamente se deberíaefectuar después de recibir la autorización apropiada.

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.

g) el mantenimiento y el copiado de las librerías fuente de programas deberían estarsujetos a un procedimiento estricto de control de cambios.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

12.5.4 Fuga de información

Control

Se deberían evitar las oportunidades para que se produzca fuga de información.

Guía de implementación

Se deberían considerar los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos:

a) exploración de los medios y comunicaciones de salida para determinar la información oculta.

b) comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.

c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408).

d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.

e) monitoreo del uso de los recursos en los sistemas de computador.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

Guía de implementación

Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativos y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

Guías de Aseguramiento

- Consultar con el personal clave buscando determinar conocimiento y conciencia de cómo las soluciones de seguridad y disponibilidad de la infraestructura serán integradas con la aplicación.
- Revisión la adquisición, implementación y planes de pruebas de la aplicación, ejecución para confirmar que se han tratado la seguridad y la disponibilidad de las aplicaciones dentro del ambiente integrado.
- Pregunte y confirme si, el diseño de la disponibilidad ha sido aprobado por autoridades técnicas.
- Revise la documentación de cierre de sesión por las partes interesadas apropiadas.
- Entrevista empresas patrocinadoras y revise la documentación para evaluar la comprensión y la adecuación del diseño de disponibilidad; comprobar si el diseño es probable que cumpla los requisitos de seguridad y disponibilidad.

AI2.5 Configuración e Implantación de Software Aplicativo Adquirido

Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio.

12.5.3 Restricciones en los cambios a los paquetes de software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) si es necesario obtener el consentimiento del vendedor.

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

Guías de Aseguramiento

- Infórmese con los propietarios de procesos y los miembros clave del negocio para determinar si sus aportes y dirección se han solicitado y reflejado en la parametrización y configuración de la aplicación. Identificar casos donde los aportes del proceso de negocios no se han solicitado.
- Confirmeconmiembrosclavedesielsoftwaredeaplicaciónesta parametrizada y configurada utilizando las mejores prácticas según lo aconsejado por los vendedores y de conformidad con estándares de la arquitectura interna.
- Inspeccione las mejores prácticas suministrados por vendedores, comparare con la estrategia de implementación, e identifiqueconfiguraciones inadecuadas.
- Confirme con los miembros clave de que los procedimientos de pruebas están implementados y cubre la verificación de cobertura de los objetivos de control de la aplicaciónadquirida (por ejemplo, la funcionalidad, interoperabilidad con las aplicaciones existentes y la infraestructura, la eficiencia desempeño de los sistemas, la integración, la capacidad de carga y pruebas de estrés, la integridad de datos).
- Inspeccione la documentación de pruebas unitarias y de integración y revise paso a paso los procedimientos de prueba para comprobar la idoneidad de las pruebas.
- Confirme con los miembros clave que todos los manuales de usuarios y de operación están completos y / o actualizado, en caso necesario. Trace una muestra de parametrización a los manuales de usuario yde operaciones para confirmar actualizaciones de la documentación.

AI2.6 Actualizaciones Importantes en Sistemas Existentes

En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y/o funcionalidad, seguir un proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos.

12.5.1 Procedimientos de control de cambios

Control

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

Guía de implementación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

a) el mantenimiento de un registro de los niveles acordados de autorización.

b) la garantía de que los cambios son realizados por los usuarios autorizados.

c) la revisión de los controles y de los procedimientos de integridad para asegurar que nose pondrán en peligro debido a los cambios.

d) la identificación de todo el software, la información, las entidades de bases de datos ydel hardware que requieran mejora.

e) la obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.

f) la garantía de que los usuarios autorizados aceptan los cambios antes de la implementación.

g) la garantía de que la documentación del sistema está actualizada al finalizar cadacambio y que la documentación antigua se archiva o elimina.

h) el mantenimiento de una versión de control para todas las actualizaciones de software.

i) el mantenimiento de un rastro para auditoría de todos los cambios solicitados.

j) la garantía de que la documentación operativa y losprocedimientos de usuario se cambian en función de la necesidad con el objeto demantener su idoneidad.

k) la garantía de que la implementación de los cambios tiene lugar en el momentooportuno y no perturba los procesos del negocio involucrados.

Guías de Aseguramiento

- Confirme con miembros clave y examine la documentación relevante para determinar que se ha realizado una evaluación del impacto de las mejoras más importantes para tratar los objetivos específicos (tales como requisito de negocio), el riesgo inherente (como los efectos en los sistemas y procesos existentes o de seguridad), la justificación de costo-beneficio y otrosrequisitos.
- Examine la documentación relevante para determinar las desviaciones del los procesos normales de desarrollo e implementación.
- Buscar informaciones de empresas patrocinadoras y otras partes afectadas e inspeccionar la documentación relevante para determinar si se ha obtenido la aprobación para el proceso del desarrollo e implementación.

AI2.7 Desarrollo de Software Aplicativo

Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el software aplicativo desarrollado por terceros.

12.5.5 Desarrollo de software contratado externamente

Control

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

Guía de implementación

Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

a) acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad.

b) certificación de la calidad y exactitud del trabajo realizado.

c) convenios de fideicomiso en caso de falla de la tercera parte.

d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado.

e) requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.

f) realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

Guías de Aseguramiento

- Confirme con los miembros clave que todas las actividades de desarrollo se han establecido para garantizar el cumplimiento de las normas de desarrollo y que el software desarrollado se basa en las especificaciones acordadas para cumplir los requerimientos funcionales y técnicos del negocio.
- Examine la documentación relevante (como el diseño, revisión de código y seguimientos detallados) para identificar excepciones a las especificaciones y a los estándares.
- Obtener y revisar la documentación de evaluaciones del software desarrollado para confirmar la suficiencia.
- Confirme con los miembros clave que las autoridades técnicas y operaciones de gestión de aplicaciones están preparadas y adecuadas para la migración al entorno de producción.
- Realizar una revisión detallada del código e identifique problemas / excepciones.
- Investigue con los miembros clave para determinar el cumplimiento con todas las obligaciones y requisitos.
- Revisar las obligaciones contractuales y los requerimientos de licenciamiento referente a los desarrollados por terceros.

AI2.8 Aseguramiento de la Calidad del Software

Desarrollar, Implementar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

Guías de Aseguramiento

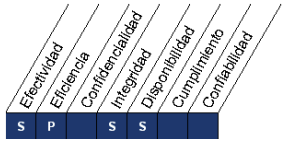
- Confirme con los miembros clave que el plan de control de calidad de software ha sido definido, incluyendo la especificación de los criterios de calidad, de los procesos de validación y verificación, y la definición de cómo la calidad será revisada.
- Revisar el plan para los criterios enumerados anteriormente, y asegúrese que las revisiones de control de calidad se llevan a cabo independientemente del equipo de desarrollo.
- Confirme con los miembros clave de que un proceso de monitoreo de calidad de software ha sido diseñado y establecido.
- Revise la documentación relevante para confirmar que el proceso se basa en los requisitos del proyecto, las políticas empresariales, procedimientos de gestión de calidad y criterios deaceptación. Confirme con los miembros clave de que todas las excepciones de calidad están identificadas yque las medidas correctivas están tomadas.
- Examine la documentación relevante de las revisiones, los resultados, las excepciones y correcciones para determinar que los exámenes de control de calidad son repetidas cuando sean necesarias.

AI3 Adquirir y Mantener Infraestructura Tecnológica

Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Recurso de TI

Criterios de Información



Gobierno de TI

AI3.2 Protección y Disponibilidad del Recurso de Infraestructura

Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Guía de implementación

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Guías de Aseguramiento

- Confirme con los miembros clave que todos los datos y el software de la infraestructura están respaldados antes de tareas de instalación y / o mantenimiento. Examine los registros de las copias de seguridad para validar lo anterior.

- Confirme con los miembros clave que todo el software de aplicación es probado antes de la instalación en un ambiente distinto al de él, pero lo suficientemente similar a, producción. Examen las especificaciones y los procedimientos de prueba para confirmar que las pruebas incluyen condiciones de funcionalidad, seguridad, disponibilidad e integridad, y todas las recomendaciones de otros proveedores.

- Revise la configuración del software para confirmar que los aspectos clavesse han tratado, incluyendo cambios de contraseñas por defecto, la configuración inicial del parámetros relativa a la seguridad y cualquier otro por defecto proveedor.

- Pregunte y confirme si, el acceso temporal concedido para su instalación se controla y si las contraseñas son cambiadas inmediatamente después que se ha completado de la instalación.Revise que los parámetros de seguridad de las aplicaciones se cumplen.

- Confirme con los miembros clave que solamente el software apropiadamente licenciado esaprobado e instalado y que las instalaciones se realizan de acuerdo conlas directrices del vendedor. Identificar los casos donde las directrices vendedor no fueron seguidas, y confirmar que fueron consultados los vendedores sobre el impacto potencial.

- Confirme con los miembros clave que existe un grupo independiente (por ejemplo, la bibliotecaria) se le concede acceso a la circulación de los programas y datos entre las bibliotecas. En su caso, revisar que el acceso del usuario al sistema de gestión de bibliotecas.

- Verifique que todos los usuarios con acceso a la gestión de software los programas de registro / salida y a los datos de las bibliotecas tengan sus formas de autorización de acceso, y confirmar la aprobación de un miembro apropiado.

- Investigue con los miembros claves si los procedimientos de aceptación se hacen cumplir usando criterios de aceptación objetivo y si los criterios de aceptación asegura que el desempeño del productoel rendimiento es consistente con las especificaciones y los requisitos acordados. Examen las especificaciones acordadas y / o requerimientos de SLA, y compararlos con los procedimientos de aceptación de la identificando las áreas donde los procedimientos no se siguen adecuadamente.

- Confirme con los miembros clave que el acceso a las actividades de mantenimiento sobre componentes sensibles de la infraestructura es registrado y revisado periódicamente por un miembro responsable de alto rangodel personal y con experiencia.

- Revisar los registros de mantenimiento y confirmar que han sido registrados todos los ítems. Examen de la documentación relevante (por ejemplo, registro de la matriz de log y la revisión periódica de la seguridad del sistemainformes) para confirmar que los registros son revisados de manera regular.**Escuchar**

Leer fonéticamente

Diccionario - Ver diccionario detallado

AI3.3 Mantenimiento de la Infraestructura

Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

9.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) el personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida.

b) se debería evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.

c) las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente.

d) no se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.

9.2.4 Mantenimiento de los equipos

Control

Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

Guía de implementación

Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos:

a) el mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.

b) sólo personal de mantenimiento autorizado debería realizar las reparaciones y el servicio de los equipos.

c) se recomienda conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo.

d) es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización; cuando sea necesario, la información sensible se debería retirar del entorno del equipo o el personal de mantenimiento debería ser suficientemente revisado.

e) se deberían cumplir todos los requisitos impuestos por las pólizas de seguros.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Guía de implementación

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación devulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización deberíaidentificar los riesgos asociados y las acciones que se han de tomar; tales accionespodrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, laacción a tomar se debería ejecutar de acuerdo con los controles relacionados con lagestión de cambios o siguiendo los procedimientos derespuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con suinstalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar queson eficaces y no producen efectos secundarios intolerables; si no hay parchedisponible, se recomienda considerar otros controles:

    1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

    2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego(*firewalls*), en las fronteras de la red.

3) aumentar el monitoreo para detectar o prevenir los ataques reales.

4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar aintervalos regulares para garantizar su eficacia y eficiencia.

j) se deberían tratar primero los sistemas con alto riesgo.

Guías de Aseguramiento

- Confirme con los miembros clave que el proceso de mantenimiento del software del sistema instalado utiliza el mismo proceso que las actualizaciones de aplicaciones, en su caso. Inspeccione el mantenimiento planificado del software del sistema e identifique las desviaciones del proceso normal para las actualizaciones de la aplicación y / o excepciones de los procedimientos y directrices proveedor.

- Confirme con los miembros clave que la documentación del software del sistema se mantiene, vigentey actualizada con la documentación del proveedor para todas las actividadesde mantenimiento del sistema.

- Inspeccione la documentación relevante e identifique áreas donde está incompleta u obsoleta.

- Infórmese con los miembros para confirmar el proceso o método utilizado para obtener la notificación oportuna de la disponibilidad de las actualizaciones de los proveedores y / o parches (por ejemplo, unacuerdo específico con el proveedor, la pertenencia a un grupo de usuarios de productos, suscripción a una revista profesional).

- Inspeccionar una muestra de software de sistema y confirmar que las actualizaciones y / o parches se han aplicado de manera oportuna.
- Identificar todas las desviaciones y / o excepciones.
- Infórmese con los miembros clave si la cantidad de mantenimientosefectuados, la vulnerabilidad a la infraestructura sin soporte, los riesgos futuros y vulnerabilidades de seguridad son revisados de forma regular.
- Realizar una evaluación de estas investigaciones y las zonas donde se tenga en cuenta los riesgos que han sido identificados por la evaluación no discutidos por los miembros del personal clave.
- Inspeccione los registros de seguimiento de mantenimiento y herramientas de respuesta para asegurar que los resultados de estos exámenes se comunicará al consejo de TI o un grupo equivalente a título oneroso en el proceso de planificación de la infraestructura.

AI3.4 Ambiente de Prueba de Factibilidad

Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad.

10.1.4 Separación de la instalaciones de desarrollo, ensayo y operación

Control

Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

Guías de implementación

Se debería identificar el grado de separación entre los ambientes operativos, de prueba y de desarrollo que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Se deberían tener presente los siguientes elementos:

a) Se recomienda definir y documentar las reglas para la transparencia de software del estado de desarrollo al operativo.

b) El software de desarrollo y el operativo se deberían ejecutar de diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.

c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando nos se requiera.

d) El ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible.

e) Los usuarios deberían emplear perfiles de usuarios diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error.

f) Los datos sensibles no se deberían copiar en el entorno del sistema de prueba.

Guías de Aseguramiento

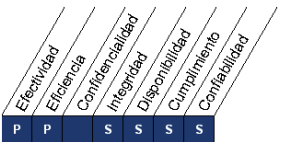
- Confirme con los miembros clave que una estrategia conmensurada con los planes estratégicos de tecnología está diseñado y que permite la creación de ambientes convenientes y prueba y simulación para ayudar a verificar la viabilidad de adquisiciones o desarrollos previstos.

AI4 Facilitar la Operación y el Uso

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.

Recurso de TI

Criterios de Información



Gobierno de TI

AI4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte

Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoyen y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

10.1.1 Documentación de los procedimientos de operación

Control

Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

Guía de implementación

Se deberían elaborar procedimientos documentados para las actividades del sistema asociadas con los servicios de comunicaciones y de procesamiento de información, como por ejemplo procedimientos para el encendido y apagado de los computadores, copias de respaldo, mantenimiento de equipos, manejo de los medios, cuarto de equipos y gestión del correo, como también de la seguridad.

Los procedimientos de operación deberían especificar las instrucciones para la ejecución detallada de cada trabajo, incluyendo:

a) procesamiento y manejo de información.

b) copias de respaldo.

c) requisitos de programación, incluyendo las interrelaciones con otros sistemas, hora de comienzo de la tarea inicial y de terminación de la tarea final.

d) instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.

e) contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

f) Instrucciones de manejo de los medios y los informes especiales, como el uso de papelería especial o el manejo de los informes confidenciales incluyendo los procedimientos para la eliminación segura de los informes de tareas fallidas.

g) procedimientos para el reinicio y la recuperación del sistema que se han de usar en caso de falla del sistema.

h) gestión de los registros de auditoría y de la información de registro del sistema.

Los procedimientos operativos, y los procedimientos documentados para las actividades del sistema, se deberían tratar como documentos formales y sus cambios deberían ser autorizados por la dirección. Cuando sea técnicamente viable, se recomienda gestionar los sistemas de información de forma consistente, utilizando los mismos procedimientos, herramientas y utilidades.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

10.7.4 Seguridad de la documentación del sistema

Control

La documentación del sistema debería estar protegida contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) la documentación del sistema se debería almacenar con seguridad.

b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.

c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

Guías de Aseguramiento

- entreviste miembros claves sobre el conocimiento del personal de operaciones y de soporte técnico para entregar, soportar y mantener con eficacia y eficientemente el sistema y la infraestructura asociada de acuerdo a los niveles de servicio (por ejemplo, entrenamiento y desarrollo de habilidades, materiales de entrenamiento, los manuales de usuario, los manuales de procedimiento, ayuda en línea, escenario de mesa de servicio).
- Revisar los materiales del entrenamiento e implementación para determinar si el proceso definido incluye el contenido requerido.
- Confirmar con entrevista con miembros clave que el personal de operaciones y soporte técnico son consientes y pueden utilizar el mecanismo de retroalimentación para determinar la suficiencia de la documentación de soporte, de los procedimientos y del entrenamiento relacionado.
- Determinar si el personal de operaciones y soporte están implicados en el desarrollo y el mantenimiento de la documentación de operaciones y soporte técnico.
- Identificar las áreas donde los procedimientos de soporte operacional no se integran con procedimientos existentes.

AI5 Adquirir Recursos de TI

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

Recurso de TI

Criterios de Información

Gobierno de TI

AI5.1 Control de Adquisición

Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI, instalaciones, hardware, software y servicios necesarios por el negocio.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

Guías de Aseguramiento

- Confirmar con entrevista a los miembros clave que proceso de adquisición de TI y la estrategia de adquisición están alineados con las políticas y los procedimientos de adquisición de la organización.
- Examine las políticas y procedimientos de gerencia del proyecto para evaluar la conformidad con las políticas y procedimientos de adquisición de la empresa.

AI5.2 Administración de Contratos con Proveedores

Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

2) Todos y los controles y mecanismos de protección física requeridos.

3) Controles para asegurar la protección contra software malicioso.

4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente. Que tienen que ver con el siguiente ítem.

7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

3) Proceso de autorización para los privilegios y el acceso de usuario.

4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad (7.2.1).

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países (15.1).

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias (15.1.2) y la protección de cualquier trabajo en colaboración (6.1.5).

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

    1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

    2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

10.8.2 Acuerdos para el intercambio

Control

Se deberían establecer acuerdos para intercambio de la información y del software entre la organización y las partes externas.

Guías de implementación

en los acuerdo de intercambio se deberían tomar en consideración las siguientes consideraciones de seguridad:

a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción.

b) Procedimientos para notificar a quien envía la transmisión, el despacho y la recepción.

c) Procedimientos para garantizar la trazabilidad y el no-repudio.

d) Normas técnicas mínimas para el empaquetado y la transmisión.

e) Acuerdos de fideicomiso.

f) Normas para identificar los servicios de mensajería.

g) Responsabilidades y deberes en caso de incidentes de seguridad de la seguridad de la información, como la pérdida de datos.

h) Uso de sistemas acordados de etiquetado de la información sensible o critica, garantizando que el significado de las etiquetas se entiendan inmediatamente y que la información está protegida adecuadamente.

i) Propiedad y responsabilidades para la protección de datos, derechos de copias, conformidad de las licencias de software y consideraciones similares.

j) Normas técnicas para registrar y leer la información y el software.

k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

Se deberían establecer y considerar políticas procedimientos y normas para proteger la información y los medios físicos en tránsito y ellos se debería referenciar en dichos acuerdos de intercambios.

El contenido sobre la seguridad de cualquier acuerdo debería reflejar la sensibilidad de la información del negocio involucrada.

12.5.5 Desarrollo de software contratado externamente

Control

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

Guía de implementación

Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

a) acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.

b) certificación de la calidad y exactitud del trabajo realizado.

c) convenios de fideicomiso en caso de falla de la tercera parte.

d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado.

e) requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.

f) realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

Guías de Aseguramiento

- confirmar a través de entrevistas con los miembros clave que las políticas y los estándares están definidos para establecer contratos con los proveedores. Las políticas y los estándares deben tratar, los aspectos legales, financieros, documentales, organizacionales, de desempeño y de alguna de las siguientes:
  - ✓ responsabilidades del proveedor
  - ✓ responsabilidades del cliente
  - ✓ SLAs del proveedor
  - ✓ Monitoree y reporte contra los SLAs
  - ✓ Acuerdos de transición
  - ✓ Procedimiento de notificación y escalamiento
  - ✓ Estándares de la seguridad, gestión de registro y requerimientos de control
  - ✓ Practicas requeridas de QA del proveedor
  - ✓ Derecho a auditar
  - ✓ Penalidades o incentivos referentes a niveles de servicios acordados
  - ✓ Derechos de propiedad intelectual
  - ✓ Provisión de aseguramiento independiente
  - ✓ Requerimientos de cláusulas de actualización de tecnología.

AI6 Administrar Cambios

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

AI6.1 Estándares y Procedimientos para Cambios

Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

10.1.2 Gestión del cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Guía de implementación

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio. En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos.

b) planificación y pruebas de los cambios.

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

d) procedimiento de aprobación formal para los cambios propuestos.

e) comunicación de los detalles del cambio a todas las personas implicadas.

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

12.5.3 Restricciones en los cambios a los paquetes de software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) si es necesario obtener el consentimiento del vendedor.

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

Guías de Aseguramiento

- Investigar y confirmar que los procesos y los procedimientos para manejar peticiones de cambio (incluyendo mantenimiento y parches) se aplican a aplicaciones, procedimientos, procesos, parámetros de sistema y servicios y a las plataformas subyacentes.

- Revisar el marco de trabajo de la gestión de cambio para determinar si el marco incluye:

- ✓ La definición de los roles y responsabilidades.
- ✓ Clasificación (por ejemplo infraestructura y aplicaciones) y priorización de todos los cambios.
- ✓ Evaluación de impacto, autorización y aprobación.
- ✓ Seguimiento de cambios.
- ✓ Mecanismo de control de versiones.
- ✓ Impacto en la integridad de los datos (por ejemplo todos los cambios a archivos de datos que son hechos bajo control de sistema y de aplicación en lugar de la intervención directa del usuario).
- ✓ Gerencia del cambio desde el inicio hasta la revisión y el cierre.
- ✓ Definición de procedimientos de rollback (retorno).
- ✓ Uso de procesos de cambios de emergencia.
- ✓ Planeación de la continuidad del negocio.
- ✓ Uso de un sistemas de gestión de registro (base de conocimiento).
- ✓ Rastros de auditoría.
- ✓ Segregación funcional.

- Investigar y confirmar si los procesos y los procedimientos para los proveedores de servicios contratados están incluidos en el proceso de gestión de cambio.
- Determinar si el proceso y los procedimientos incluye los términos contractuales y SLAs.

AI6.2 Evaluación de Impacto, Priorización y Autorización

Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

10.1.2 Gestión del cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Guía de implementación

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio. En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos.

b) planificación y pruebas de los cambios.

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

d) procedimiento de aprobación formal para los cambios propuestos.

e) comunicación de los detalles del cambio a todas las personas implicadas.

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

12.5.1 Procedimientos de control de cambios

Control

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

Guía de implementación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

a) el mantenimiento de un registro de los niveles acordados de autorización.

b) la garantía de que los cambios son realizados por los usuarios autorizados.

c) la revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.

d) la identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.

e) la obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.

f) la garantía de que los usuarios autorizados aceptan los cambios antes de la implementación.

g) la garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.

h) el mantenimiento de una versión de control para todas las actualizaciones de software.

i) el mantenimiento de un rastro para auditoría de todos los cambios solicitados.

j) la garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.

k) la garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

12.5.3 Restricciones en los cambios a los paquetes de software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) si es necesario obtener el consentimiento del vendedor.

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

   1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

   2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red.

   3) aumentar el monitoreo para detectar o prevenir los ataques reales.

   4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos

j) regulares para garantizar su eficacia y eficiencia.

k) se deberían tratar primero los sistemas con alto riesgo.

Guías de Aseguramiento

- Investigar y confirmar si el proceso de gestión de cambio permite que los dueños del proceso de negocio y TI soliciten cambios a la infraestructura, los sistemas o las aplicaciones.
- Investigar y confirmar que las solicitudes de cambio están categorizadas (infraestructura, sistemas operativos, redes y aplicaciones).

- Confirmar a través de entrevistas con miembros clave que se le da prioridad a las solicitudes de cambio basado en los criterios predefinidos (por ejemplo necesidades técnicas y de negocio para el cambio, requerimientos legales, regulatorios y contractuales).

- Investigar y confirmar que las solicitudes de cambio son evaluadas y documentadas usando un método estructurado que involucra el análisis de impacto en la infraestructura, los sistemas y las aplicaciones.

- Investigar y confirmar que las aplicaciones de seguridad, legales, contractuales y de cumplimiento son consideradas en el proceso de evaluación de la solicitud de cambio y que los dueños del negocio con involucrados.

- Investigar y confirmar que cada solicitud de cambio es aprobado formalmente por los dueños del proceso de negocio y los involucrados técnicos de TI.

- Examinar una muestra representativa de solicitudes de cambio para asegurarse de que fueron evaluados, priorizados y revisados apropiadamente.

AI6.3 Cambios de Emergencia

Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

10.1.2 Gestión del cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Guía de implementación

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio. En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos.

b) planificación y pruebas de los cambios.

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

d) procedimiento de aprobación formal para los cambios propuestos.

e) comunicación de los detalles del cambio a todas las personas implicadas.

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

11.5.4 Uso de las utilidades del sistema

Control

Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

Guía de aplicación

Se recomienda considerar la siguiente directriz para el uso de las utilidades del sistema:

a) uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.

b) separación de las utilidades del sistema del software de aplicaciones.

c) limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.

d) autorización del uso ad hoc de las utilidades del sistema

e) limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado.

f) registro de todo uso de las utilidades del sistema.

g) definición y documentación de los niveles de autorización para las utilidades del sistema.

h) retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.

i) no poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

12.5.1 Procedimientos de control de cambios

Control

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

Guía de implementación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

a) el mantenimiento de un registro de los niveles acordados de autorización.

b) la garantía de que los cambios son realizados por los usuarios autorizados.

c) la revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.

d) la identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.

e) la obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.

f) la garantía de que los usuarios autorizados aceptan los cambios antes de la implementación.

g) la garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.

h) el mantenimiento de una versión de control para todas las actualizaciones de software.

i) el mantenimiento de un rastro para auditoría de todos los cambios solicitados.

j) la garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.

k) la garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

12.5.3 Restricciones en los cambios a los paquetes de software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) si es necesario obtener el consentimiento del vendedor.

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red.

3) aumentar el monitoreo para detectar o prevenir los ataques reales.

4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos

j) regulares para garantizar su eficacia y eficiencia.

k) se deberían tratar primero los sistemas con alto riesgo.

Guías de Aseguramiento

- Investigar y confirmar que el proceso general de la gestión del cambio incluye los procedimientos de cambios de emergencia (por ejemplo definición, inicio, prueba, documentación, evaluación y autorización de cambios de emergencia).
- Examinar la documentación de una muestra representativa de cambios de emergencia y, entrevistándose con los miembros clave, establezca si los cambios de emergencia están ejecutados según lo especificado en el proceso de la gestión de cambio.
- Confirmar a través de entrevistas con los miembros clave que los arreglos de acceso de emergencia son autorizados, documentados y revocados después de que se haya aplicado el cambio.
- Investigar y confirmar que una revisión post implementación de los cambios de emergencia es conducida.

AI6.4 Seguimiento y Reporte del Estatus de Cambio

Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

10.1.2 Gestión del cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Guía de implementación

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio. En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos.

b) planificación y pruebas de los cambios.

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

d) procedimiento de aprobación formal para los cambios propuestos.

e) comunicación de los detalles del cambio a todas las personas implicadas.

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

Guías de Aseguramiento

- Investigar y confirmar si existe un proceso establecido para permitir que los solicitantes y los interesados sigan el estado de solicitudes a través de las varias etapas del proceso de gestión de cambio.
- Investigar y confirmar que el sistema de seguimiento y reporte monitorea el estado de la solicitud de cambio (por ejemplo rechazado, aprobado pero no iniciado, aprobado, en proceso).
- Investigar y confirmar que la gerencia revisa y monitorea el estado detallado de los cambios y del estado total.
- Investigar y confirmar que los cambios son aprobados en el momento oportuno y si está abiertos o cerrados,dependiendo de la prioridad.

AI6.5 Cierre y Documentación del Cambio

Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

10.1.2 Gestión del cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Guía de implementación

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio. En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos.

b) planificación y pruebas de los cambios.

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.

d) procedimiento de aprobación formal para los cambios propuestos.

e) comunicación de los detalles del cambio a todas las personas implicadas.

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

Guías de Aseguramiento

- Investigar y confirmar que la documentación de cambios (por ejemplo procedimientos operacionales, información de configuraciones, documentación de aplicación pantallas de ayuda y material de entrenamiento) es actualizada.

- Investigar y confirmar que la documentación de cambios (por ejemplo documentación de usuario y sistema de antes y después del cambio) es almacenada y retenida.

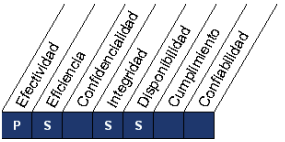
- Investigar y confirmar que la documentación del proceso de negocio es actualizada por los cambios implementados en hardware y software.

AI7 Instalar y Acreditar Soluciones y Cambios

Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados.

Recurso de TI

Criterios de Información



Gobierno de TI

AI7.1 Entrenamiento

Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de sistemas de la información de desarrollo, implementación o modificación.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Investigary confirmar si, el plan de formación es parte del plan maestro del proyecto global de los proyectos de desarrollo.
- Investigary confirmar si, (por ejemplo, a través de entrevistas con miembros clave del personal o la inspección del plan del proyecto) se identifica el plan de formación y losgruposde direcciones afectadas(por ejemplo, los usuarios finales, las operaciones de TI, soporte y capacitación de desarrollo de aplicaciones de TI, proveedores de servicios).
- Investigar y confirmar si, las estrategias alternativas de formación se consideran y que garantizan que existe una relación coste-eficacia que se ha seleccionado e incorporado en la formación marco.
- Investigar y confirmar si,hay un proceso para verificar el cumplimiento del plan de formación.
- Inspeccione la documentación de capacitación para determinar el cumplimiento del plan de formación (por ejemplo, la lista de los funcionarios invitados a los entrenamientos, lista de participantes, formularios de evaluación para ellogro de los objetivos de aprendizaje y otras opiniones).

- Investigar y confirmar si, hay un proceso de control del entrenamiento para aprovechar la información que podría conducir a posibles mejoras en el sistema.
- Investigary confirmar si, los cambios previstos son monitoreadosy se crean planes para asegurar que las necesidades de formación se consideran de manera adecuada.

AI7.2 Plan de Prueba

Establecer un plan de pruebas basado en los estándares de la organización que define roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan está aprobado por las partes relevantes.

12.5.1 Procedimientos de control de cambios

Control

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

Guía de implementación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

a) el mantenimiento de un registro de los niveles acordados de autorización.

b) la garantía de que los cambios son realizados por los usuarios autorizados.

c) la revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.

d) la identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.

e) la obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.

f) la garantía de que los usuarios autorizados aceptan los cambios antes de la implementación.

g) la garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.

h) el mantenimiento de una versión de control para todas las actualizaciones de software.

i) el mantenimiento de un rastro para auditoría de todos los cambios solicitados.

j) la garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.

k) la garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

Guías de Aseguramiento

- Investigary confirmar si, hay un plan de prueba desarrollado y documentado en conformidadcon el plan de calidad del proyecto y las normas de la organización y que se comunica a los propietarios del negocios y las partes interesadas de la información de manera adecuada.
- Investigar y confirmar si, el plan de ensayo refleja la evaluación de los riesgos del proyecto y que todos los requisitos de las pruebas funcionales y técnicas se incluyen.

- Investigar y confirmar si, en el plan de pruebas se determinan los recursos para ejecutar las pruebas y evaluar los resultados de las pruebas.
- Confirme que los participantes son consultados sobre las repercusiones financieras del plan de pruebas.
- Investigary confirmar si, el plan de ensayo considera la preparación de exámenes, incluyendo la preparación del sitio, las necesidades de formación, instalación o actualización de un ensayo que se definenmedio ambiente, la planificación / performance / documentación / retención de casos de prueba, error y manipulación problema, la corrección y la progresividad, y su aprobación oficial.
- Para una muestra de los planes de prueba, inspeccionar la documentación para determinar si las fases de las pruebas relevantes se llevan a cabo.
- Investigar y confirmar si, el plan de ensayos establece criterios precisos para medir el éxito de llevar a cabo cada fase de la prueba y que las consultas con los propietarios de los procesos de negocio y las partes interesadas de TI son considerados en la definición de los criterios de éxito.
- Determinar si el plan establece los procedimientos de remediación cuando los criterios de éxito no se cumplen (por ejemplo, en caso de fallas significativas en una fase de prueba, el plan se dan orientaciones sobre si se debe proceder a la siguiente fase, detener o aplazar la aplicación de pruebas).
- Investigary confirmar si, los planes de prueba son aprobados por las partes interesadas, incluidos los propietarios de procesos del negocio y de TI, según corresponda. Ejemplos de otras partes interesadas son gerentes de desarrollo de aplicaciones, gestores de proyectos y usuarios finales de procesos del negocio.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

AI7.4 Ambiente de Prueba

Definir y establecer un entorno seguro de pruebas representativo del entorno de operaciones planeado relativo a seguridad, controles internos, practicas operativos, calidad de los datos y requerimientos de privacidad, y cargas de trabajo.

10.1.4 Separación de la instalaciones de desarrollo, ensayo y operación

Control

Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

Guías de implementación

Se debería identificar el grado de separación entre los ambientes operativos, de prueba y de desarrollo que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Se deberían tener presente los siguientes elementos:

a) Se recomienda definir y documentar las reglas para la transparencia de software del estado de desarrollo al operativo.

b) El software de desarrollo y el operativo se deberían ejecutar de diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.

c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando nos se requiera.

d) El ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible.

e) Los usuarios deberían emplear perfiles de usuarios diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error.

f) Los datos sensibles no se deberían copiar en el entorno del sistema de prueba.

12.4.3 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implementación

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas, con el objeto de reducir el potencial de corrupción de los programas de computador:

a) cuando sea posible, las librerías fuente de programas no se deberían mantener en los sistemas operativos.

b) el código fuente de programas y las librerías fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.

c) el personal de soporte debería tener acceso restringido a las librerías fuente de programas.

d) la actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.

g) el mantenimiento y el copiado de las librerías fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

Guías de Aseguramiento

- Pregunte y confirmesi, el entorno de prueba se configura para reflejar el entorno de producción (factores incluyen la carga de trabajo / estrés, sistemas operativos, software de aplicación necesarias, los sistemas de gestión de bases de datos, infraestructura de redes y computación).
- Pregunte y confirmesi, el entorno de prueba no es capaz de interactuar con los entornos de producción.
- Investigar y confirmar si, existe una base de datos de prueba.
- Evaluar la existencia y la calidad de un proceso de desinfección de datos en la creación de una base de datos de prueba.
- Evaluar las medidas de protección y la autorización de acceso al entorno de prueba.
- Investigary confirmar si, existe un proceso para gestionar la conservación o la eliminación de los resultados de las pruebasy se cumpla.
- Investigary confirmar si, el proceso de retención cumple o excede los requisitos reglamentarios o de cumplimiento.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

AI7.6 Pruebas de Cambios

Pruebas de cambios independientemente en acuerdo con los planes de pruebas definidos antes de la migración al entorno de operaciones. Asegurar que el plan considera la seguridad y el desempeño.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

12.4.3 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implementación

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas, con el objeto de reducir el potencial de corrupción de los programas de computador:

a) cuando sea posible, las librerías fuente de programas no se deberían mantener en los sistemas operativos.

b) el código fuente de programas y las librerías fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.

c) el personal de soporte debería tener acceso restringido a las librerías fuente de programas.

d) la actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.

g) el mantenimiento y el copiado de las librerías fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

Guías de Aseguramiento

- Investigary confirmar si, las pruebas de los cambios se desarrolla con la independencia (separación de funciones) y es llevada a cabo sólo en el entorno de prueba.
- Investigary confirmar si, existen scripts de prueba para validar la seguridad y el rendimiento.
- Confirmar a través de entrevistas que los planes de emergencia o backout se elaborarán y probarán antes que los cambios sean promovidosa producción.

AI7.7 Prueba de Aceptación Final.

Asegurar que el dueño de proceso de negocio y los interesados de TI evalúan los resultados de los procesos de pruebas como determina el plan de pruebas. Remediar los errores significativos identificados en el proceso de pruebas, habiendo completado el conjunto de pruebas identificadas en el plan de pruebas y cualquier prueba de regresión necesaria. Siguiendo la evaluación, aprobación promoción a producción.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal.se deberían considerar los siguientes elementos antes de la aceptación formal:

a) Requisitos de desempeño y capacidad de los computadores.

b) Procedimientos de reinicio y de recuperación por errores y planes de contingencia.

c) Preparación y prueba de procedimientos operativos de una rutina para las normas definidas.

d) Establecimiento del conjunto de controles de seguridad acordados.

e) Procedimientos manuales eficaces.

f) Disposiciones para la continuidad del negocio.

g) Evidencia de que la instalación del sistema nuevo no afectara adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final del mes.

h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.

i) Formación en el funcionamiento o utilización de los sistemas nuevos.

j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

12.5.4 Fuga de información

Control

Se deberían evitar las oportunidades para que se produzca fuga de información.

Guía de implementación

Se deberían considerar los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos:

a) exploración de los medios y comunicaciones de salida para determinar la información oculta.

b) comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.

c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408).

d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.

e) monitoreo del uso de los recursos en los sistemas de computador.

Guías de Aseguramiento

- Confirme que los principales interesados son considerados en las actividades de prueba de aceptación final.
- Pregunte y confirmesi, en las etapas de recepción definitiva, criterios de éxito son identificados en el plan de pruebas.
- Investigary confirmar si, la documentación es apropiada para su revisión y evaluación existe.
- Infórmese de las partes interesadas clave si la documentación y presentación de los resultados finales de las pruebas de aceptación son completas y oportunas.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

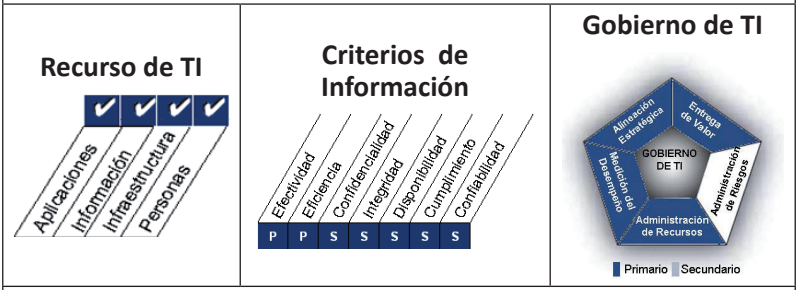
APÉNDICE C

GUÍAS PARA EL DOMINIO DE ENTREGA Y SOPORTE

ENTREGAR Y SOPORTE (DS)

DS1Definir y Administrar los Niveles de Servicio

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicaciónefectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye elmonitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este procesopermite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.



DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio

Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de-servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita elentendimiento común entre el cliente y el(los) prestador(es) de servicio.

El marco de trabajo incluye procesos para la creación derequerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) ylas fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructuraorganizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedoresexternos e internos y de los clientes.

10.2.1 Prestación del servicio

Control

Se deberían garantizar que los controles de seguridad, las definiciones del servicio y los nivelesde prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operadospor el tercero.

Guía de implementación

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones deseguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso decontrataciones externas, la organización debería planificar las transiciones necesarias (deinformación, servicios de procesamiento de información y todo lo demás que se deba transferir)y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que el tercero mantenga una capacidad deservicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación delos niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio.

Guías de Aseguramiento

- Inspeccione SLA, políticas y procedimientos para la alineación de los objetivos de SLA y medidas de desempeño con los objetivos de negocio y estrategia de TI.

- Averiguar y confirmar si las políticas existen para la alineación de los objetivos de SLA y medidas de desempeño con los objetivos de negocio y estrategia de TI.
- Inspeccione el catálogo de servicios y verificar que incorpora los requisitos de servicio, las definiciones de servicio, SLA, OLA y fuentes de financiación.
- Infórmese de los funcionarios responsables de la escala de SLA y la resolución para determinar si los procedimientos o métodos establecidos de servicios están dentro de los niveles razonables en responder a los problemas.
- Inspeccionar una muestra de los cambios pertinentes y verificar que los cambios se llevaron a cabo de conformidad con el proceso de gestión del cambio.
- Inspeccione el diseño del programa de mejora de servicios de los estándares para medir el desempeño.

DS1.2 Definición de Servicios

Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados yalmacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

10.2.1 Prestación del servicio

Control

Se deberían garantizar que los controles de seguridad, las definiciones del servicio y los nivelesde prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operadospor el tercero.

Guía de implementación

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones deseguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso decontrataciones externas, la organización debería planificar las transiciones necesarias (deinformación, servicios de procesamiento de información y todo lo demás que se deba transferir)y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que el tercero mantenga una capacidad deservicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación delos niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio.

Guías de Aseguramiento

- Averiguar y confirmar si existe un proceso de desarrollo, revisión y ajuste del catálogo de servicios o de la cartera de servicios.
- Confirmar la existencia de un proceso de gestión para asegurar que el catálogo de servicios o de la cartera está disponible, completa y actualizada.
- Inspeccione el proceso de catálogo de servicios o de la cartera para comprobar que se revisa de manera regular.Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS1.3 Acuerdos de Niveles de Servicio

Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente ylas capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas ycuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y definanciamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad,confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones dedemanda.

10.2.1 Prestación del servicio

Control

Se deberían garantizar que los controles de seguridad, las definiciones del servicio y los nivelesde prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operadospor el tercero.

Guía de implementación

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones deseguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso decontrataciones externas, la organización debería planificar las transiciones necesarias (deinformación, servicios de procesamiento de información y todo lo demás que se deba transferir)y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que el tercero mantenga una capacidad deservicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación delos niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio.

Guías de Aseguramiento

- Averiguar y confirmar si los interesados de acuerdo de SLA, en registrar y comunicar, y lo queestá incluido en el formato y el contenido.
- Inspeccione el formato del contenido del SLA para verificar que se incluye exclusiones, los acuerdos comerciales y OLA.
- Inspeccione el proceso de gestión de SLA para verificar que las medidas de SLA (cualitativos y cuantitativos) y los objetivos del SLA son monitoreados.
- Inspeccione los SLA para su aprobación y firma correspondiente.
- Observar y examinar el proceso de revisión de SLA para evaluar su idoneidad.
- Verifique que el proceso de mejoras o ajustes a los SLA se basa en la retroalimentación sobre el desempeño y los cambios en los requisitos del cliente y del negocio.
- Infórmese de los funcionarios clave si los servicios están siendo prestados que no están documentados en el SLA. Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio

Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento delos niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo sonanalizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

10.2.2 Monitoreo y revisión de los servicios por terceros

Control

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares.

Guía de implementación

El monitoreo y la revisión de los servicios por terceros deberían garantizar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos y que los incidentes y problemas de la seguridad de la información se manejan adecuadamente. Ello debería implicar una relación y un proceso de gestión del servicio entre la organización y el tercero para:

a) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos.

b) Revisar los reportes del servicio elaborados por el tercero y acordar reuniones periódicas sobre el progreso, según lo exijan los acuerdos.

c) Suministrar información sobre los incidentes de seguridad de la información, y revisión de esta información por parte de la organización y el tercero, según lo exijan los acuerdos, directrices y los procedimientos de soporte.

d) Revisión de los registros y pruebas de auditoría del tercero con respecto a eventos de seguridad, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado.

e) Resolver y manejar todos los problemas identificados.

La responsabilidad por la gestión de la relación con el tercero se le debería asignar a una persona o a un equipo de gestión del servicio. Además, la organización debería garantizar que el tercero asigna responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos. Se recomienda poner a disposición suficientes habilidades técnicas y recursos para monitorear el cumplimiento de los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Cuando se observan deficiencias en la prestación del servicio se deberían tomar las acciones adecuadas.

La organización debería mantener suficiente control global y no perder de vista todos los aspectos de seguridad para la información sensible o crítica, o de los servicios de procesamiento de información que haya procesado, gestionado o tenido acceso el tercero. La organización debería asegurarse de que conserva visibilidad en las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades e informe / respuesta de los incidentes de seguridad de la información a través de un proceso, estructuras y formatos definidos claramente para la presentación de informes.

10.2.3 Gestión de los cambios en los servicios por terceras partes

Control

Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de laspolíticas existentes de seguridad de la información, en los procedimientos y los controles sedeberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocioinvolucrados, así como la reevaluación de los riesgos.

Guía de implementación

Es necesario que el proceso de gestión de los cambios en el servicio prestado por el tercerotome en consideración:

a) los cambios hechos por la organización para implementar:

   1) mejoras en los servicios actuales ofrecidos.

   2) desarrollo de todos los sistemas o aplicaciones nuevas.

   3) modificaciones o actualizaciones de las políticas y procedimientos de la organización.

   4) controles nuevos para resolver los incidentes de seguridad de la información y para mejorar la seguridad.

b) cambios en los servicios por el tercero para implementar:

   1) cambios y mejoras en las redes.

   2) uso de nuevas tecnologías.

   3) adopción de productos nuevos o versiones / divulgaciones más recientes.

   4) nuevas herramientas y entornos de desarrollo.

   5) cambios en la ubicación física de las instalaciones de los servicios.

   6) cambio de proveedores.

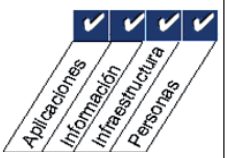
Guías de Aseguramiento

- A través de entrevistas con miembros clave del personal responsable de la supervisión del rendimiento de nivel de servicio, determinar los criterios de presentación de informes.
- Obtener muestras de informes sobre el rendimiento del SLA, y verificar la distribución.
- Inspeccione los comentarios sobre previsiones y tendencias en el rendimiento de nivel de servicio.
- Diccionario - Ver diccionario detallado

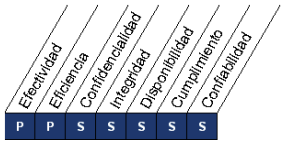
DS2 Administrar los Servicios de Terceros

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de unproceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades yexpectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichosacuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores queno se desempeñan de forma adecuada.

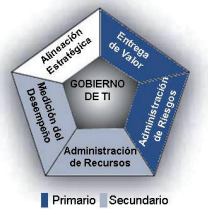
Recurso de TI



Criterios de Información



Gobierno de TI



DS2.1 Identificación de Todas las Relaciones con Proveedores

Identificar todos los servicios de los proveedores, y categorizar los de acuerdo al tipo de proveedor, significado y criticidad. Mantenerdocumentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregablesesperados, y credenciales de los representantes de estos proveedores.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

   1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

   2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

   3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

   4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

Guías de Aseguramiento

- Averiguar y confirmar si un registro de las relaciones con los proveedores se mantiene. Obtener y revisar los criterios de relación con proveedores de razonabilidad e integridad de las categorizaciones de provisión de tipos, importancia y criticidad.

- Determinar si el esquema de categorización proveedor es lo suficientemente detallada para clasificar todas las relaciones con los proveedores sobre la base de la naturaleza de los servicios contratados.

- Compruebe si historias pasadas en la selección / rechazo del proveedor son conservados y utilizados.

- Inspeccionar el registro de relaciones con los proveedores para asegurarse de que está al día, debidamente clasificados y suficientemente detallada para asegurarse de que proporciona una base para control de los proveedores existentes.

- Inspeccionar una muestra representativa de contratos de proveedores, SLAs y otros documentos para garantizar que se corresponden con el registro de proveedores.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS2.2 Gestión de Relaciones con Proveedores

Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar lascuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (Ej.: a través deSLAs).

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

   4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

3) Proceso de autorización para los privilegios y el acceso de usuario.

4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

   1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

   2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

   3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

10.2.3 Gestión de los cambios en los servicios por terceras partes

Control

Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de laspolíticas existentes de seguridad de la información, en los procedimientos y los controles sedeberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocioinvolucrados, así como la reevaluación de los riesgos.

Guía de implementación

Es necesario que el proceso de gestión de los cambios en el servicio prestado por el tercerotome en consideración:

a) los cambios hechos por la organización para implementar:

   1) mejoras en los servicios actuales ofrecidos.

   2) desarrollo de todos los sistemas o aplicaciones nuevas.

   3) modificaciones o actualizaciones de las políticas y procedimientos de la organización.

   4) controles nuevos para resolver los incidentes de seguridad de la información y para mejorar la seguridad.

b) cambios en los servicios por el tercero para implementar:

   1) cambios y mejoras en las redes.

   2) uso de nuevas tecnologías.

   3) adopción de productos nuevos o versiones / divulgaciones más recientes.

   4) nuevas herramientas y entornos de desarrollo.

   5) cambios en la ubicación física de las instalaciones de los servicios.

   6) cambio de proveedores.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

Guías de Aseguramiento

- Inspeccione el servicio de documentación de proveedores para las pruebas de los roles formales y responsabilidades, y determinar si las funciones de gestión de proveedores se han documentado ycomunicadas dentro de la organización.

- Determinar si existen políticas para hacer frente a la necesidad de contratos formales, la definición del contenido de los contratos, y la asignación de responsabilidades gerente propietario o de la relaciónpara garantizar que los contratos se crea, mantiene, seguimiento y renegociado cuando sea necesario.

- Evaluar si la asignación de las funciones de gestión de proveedores es razonable y se basa en el nivel y los conocimientos técnicos necesarios para gestionar con eficacia la relación.

DS2.3 Administración de Riesgos del Proveedor

Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega deforma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legalesy regulatorios de los estándares universales del negocio. La administración del riesgo debe considerar además acuerdos deconfidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos deseguridad, proveedores alternativos, penalizaciones e incentivos, etc.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

   4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

   5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

   6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

   7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

   1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

   2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

   3) Proceso de autorización para los privilegios y el acceso de usuario.

   4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

   5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

   6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

8.1.2 Selección

Control

Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Guías de implementación

En las revisiones de verificación se deberían tener en cuenta la legislación pertinente a la privacidad, la protección de datos personales y / o el empleo y cuando se permite, debería incluir lo siguiente:

a) Disponibilidad de referencia de comportamiento satisfactorio, por ejemplo una laboral y otra personal.

b) Una verificación (para determinar la totalidad y exactitud) de la hoja de vida del candidato.

c) Confirmación de las calificaciones profesionales y académicas declaradas.

d) Verificación de la identidad independiente (pasaporte o documento similar)

e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible, como por ejemplo información financiera o de alta confidencialidad, la organización debería considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y las limitaciones para las revisiones de verificación, por ejemplo quien es elegible para seleccionar al personal y cómo, cuándo y por qué se realizan las verificaciones.

También deberían llevar a cabo un proceso de selección para los contratistas y los usuarios de terceras partes. Cuando los contratistas son suministrados por una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para la selección y los procedimientos de notificación que es necesario seguir si la selección no se ha completado o si los resultados arrojan dudas o preocupación. De la misma manera, el acuerdo de la tercera parte debería especificar claramente todas las responsabilidades y los procedimientos de la notificación para la selección.

Informar sobre todos los candidatos que se consideran para los cargos dentro de la organización se debería recolectar y manejar según la legislación adecuada existente en la jurisdicción correspondiente.

Dependiendo de la legislación que se aplique, se debería informar con anticipación a los candidatos sobre las actividades de selección.

8.1.3 Términos y condiciones laborales

Control

Como parte de la obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual deber establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

Guías de implementación

Los términos y condiciones laborales deberían refleja la política de seguridad de la organización, además debería aclarar y establecer:

a) Que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a la información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información.

b) Los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o legislación sobre protección de datos.

c) Responsabilidades para la clasificación de la información y la gestión de los activos asociados con sistemas y servicios de información manejados por el empleado, el contratista o usuario de tercera parte.

d) Responsabilidades del empleado, contratista o usuario de tercera parte para el manejo de información recibida de otras empresas o de partes externas.

e) Responsabilidades de la organización para el manejo de la información personal, incluyendo la información personal creada como resultado o durante el contrato laboral con la organización.

f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio.

g) Acciones a tomar si el empleado, contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

La organización debería garantizar que los empleados, los contratistas y los usuarios de terceras partes están de acuerdo con los términos y condiciones respecto a la seguridad de la información según la naturaleza del acceso que tendrán a los activos de la organización asociado con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones laborales deberían durante un periodo definido después de la terminación del contrato laboral (8.3).

10.2.3 Gestión de los cambios en los servicios por terceras partes

Control

Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de laspolíticas existentes de seguridad de la información, en los procedimientos y los controles sedeberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocioinvolucrados, así como la reevaluación de los riesgos.

Guía de implementación

Es necesario que el proceso de gestión de los cambios en el servicio prestado por el tercerotome en consideración:

a) los cambios hechos por la organización para implementar:

   1) mejoras en los servicios actuales ofrecidos.

   2) desarrollo de todos los sistemas o aplicaciones nuevas.

   3) modificaciones o actualizaciones de las políticas y procedimientos de la organización.

   4) controles nuevos para resolver los incidentes de seguridad de la información y para mejorar la seguridad.

b) cambios en los servicios por el tercero para implementar:

1) cambios y mejoras en las redes.

2) uso de nuevas tecnologías.

3) adopción de productos nuevos o versiones / divulgaciones más recientes.

4) nuevas herramientas y entornos de desarrollo.

5) cambios en la ubicación física de las instalaciones de los servicios.

6) cambio de proveedores.

10.8.2 Acuerdos para el intercambio

Control

Se deberían establecer acuerdos para intercambio de la información y del software entre la organización y las partes externas.

Guías de implementación

en los acuerdo de intercambio se deberían tomar en consideración las siguientes consideraciones de seguridad:

a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción.

b) Procedimientos para notificar a quien envía la transmisión, el despacho y la recepción.

c) Procedimientos para garantizar la trazabilidad y el no-repudio.

d) Normas técnicas mínimas para el empaquetado y la transmisión.

e) Acuerdos de fideicomiso.

f) Normas para identificar los servicios de mensajería.

g) Responsabilidades y deberes en caso de incidentes de seguridad de la seguridad de la información, como la pérdida de datos.

h) Uso de sistemas acordados de etiquetado de la información sensible o critica, garantizando que el significado de las etiquetas se entiendan inmediatamente y que la información está protegida adecuadamente.

i) Propiedad y responsabilidades para la protección de datos, derechos de copias, conformidad de las licencias de software y consideraciones similares.

j) Normas técnicas para registrar y leer la información y el software.

k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

Se deberían establecer y considerar políticas procedimientos y normas para proteger la información y los medios físicos en tránsito y ellos se debería referenciar en dichos acuerdos de intercambios.

El contenido sobre la seguridad de cualquier acuerdo debería reflejar la sensibilidad de la información del negocio involucrada.

Guías de Aseguramiento

- Averiguar si los riesgos asociados con la incapacidad de cumplir con los contratos de proveedores se definen.
- Averiguar si los recursos fueron considerados en la definición del contrato de abastecimiento.
- Inspeccione el contrato de la documentación de evidencia de la revisión.
- Infórmese de los funcionarios clave de si un proceso de gestión del riesgo que existe para identificar y monitorear los riesgos de proveedores.
- Determinar si las políticas que exigen la independencia en el abastecimiento de proveedores y el proceso de selección, y entre el personal de los proveedores y la gestión dentro de laorganización.

DS2.4 Monitoreo del Desempeño del Proveedor

Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con losrequerimientos del negocio actuales y que se adhiere continuamente a los acuerdos del contrato y a SLAs, y que el desempeño escompetitivo con proveedores alternativos y las condiciones del mercado.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

    1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

2) Todos y los controles y mecanismos de protección física requeridos.

3) Controles para asegurar la protección contra software malicioso.

4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

3) Proceso de autorización para los privilegios y el acceso de usuario.

4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

    1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

    2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

    3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

10.2.1 Prestación del servicio

Control

Se deberían garantizar que los controles de seguridad, las definiciones del servicio y los nivelesde prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operadospor el tercero.

Guía de implementación

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones deseguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso decontrataciones externas, la organización debería planificar las transiciones necesarias (deinformación, servicios de procesamiento de información y todo lo demás que se deba transferir)y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que el tercero mantenga una capacidad deservicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación delos niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio.

10.2.2 Monitoreo y revisión de los servicios por terceros

Control

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar yrevisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares.

Guía de implementación

El monitoreo y la revisión de los servicios por terceros deberían garantizar el cumplimiento delos términos y condiciones de seguridad de la información de los acuerdos y que los incidentesy problemas de la seguridad de la información se manejan adecuadamente. Ello deberíaimplicar una relación y un proceso de gestión del servicio entre la organización y el terceropara:

a) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos.

b) Revisar los reportes del servicio elaborados por el tercero y acordar reuniones periódicas sobre el progreso, según lo exijan los acuerdos.

c) Suministrar información sobre los incidentes de seguridad de la información, y revisión de esta información por parte de la organización y el tercero, según lo exijan los acuerdos, directrices y los procedimientos de soporte.

d) Revisión de los registros y pruebas de auditoría del tercero con respecto a eventos de seguridad, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado.

e) Resolver y manejar todos los problemas identificados.

La responsabilidad por la gestión de la relación con el tercero se le debería asignar a unapersona o a un equipo de gestión del servicio. Además, la organización debería garantizar queel tercero asigna responsabilidades para la verificación del cumplimiento y la aplicación de losrequisitos de los acuerdos. Se recomienda poner a disposición suficientes habilidades técnicasy recursos para monitorear el cumplimiento de los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Cuando se observandeficiencias en la prestación del servicio se deberían tomar las acciones adecuadas.

La organización debería mantener suficiente control global y no perder de vista todos losaspectos de seguridad para la información sensible o crítica, o de los servicios deprocesamiento de información que haya procesado, gestionado o tenido acceso el tercero. Laorganización debería asegurarse de que conserva visibilidad en las actividades de seguridadcomo gestión de cambios, identificación de vulnerabilidades e informe / respuesta de losincidentes de seguridad de la información a través de un proceso, estructuras y formatosdefinidos claramente para la presentación de informes.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Guía de implementación

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

12.5.5 Desarrollo de software contratado externamente

Control

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

Guía de implementación

Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

a) acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.

b) certificación de la calidad y exactitud del trabajo realizado.

c) convenios de fideicomiso en caso de falla de la tercera parte.

d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado.

e) requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.

f) realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

Guías de Aseguramiento

- Seleccionar una muestra de facturas de proveedores, determinar si se identifican los cargos por servicios contratados, según lo especificado en los contratos de servicios, y evaluar la razonabilidad de gastos en comparación con el rendimiento diversos comparables interna, externa y la industria.
- Inspeccionar una muestra de informes de los servicios de proveedores para determinar si el proveedor informa periódicamente sobre acordado los criterios de rendimiento y si la presentación de informes de rendimiento es el objetivo y cuantificables y alineados con los SLA definidos y el contrato de proveedor.

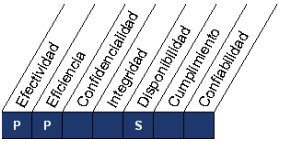
Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS3 Administrar el Desempeño y la Capacidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente eldesempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en losrequerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos deinformación que soportan los requerimientos del negocio están disponibles de manera continua.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS3.1 Planeación del Desempeño y la Capacidad

Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar ladisponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como sedetermina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelo apropiadas para producir unmodelo de desempeño, de capacidad y de desempeño de los recursos de TI, tanto actual como pronosticado.

10.3.1 Gestión de la capacidad

Control

Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones delos requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

Guía de implementación

Para cada actividad nueva y existente es conveniente identificar los requisitos de la capacidad.Se recomienda monitorear y adaptar el sistema para garantizar y, cuando sea necesario,mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles deindagación para indicar los problemas en el momento oportuno. En las proyecciones de losrequisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos delsistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento deinformación de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requierecostos elevados; por lo tanto, los directores deberían monitorear la utilización de los recursosclaves del sistema. También deberían identificar las tendencias del uso, particularmente enrelación con las aplicaciones del negocio o las herramientas del sistema de información para lagestión.

Es conveniente que los directores utilicen esta información para identificar y evitar posiblescuellos de botella así como la dependencia de personal clave, los cuales pueden presentar unaamenaza para los servicios o la seguridad del sistema, y para planificar la acción adecuada.

Guías de Aseguramiento

- Averiguar y confirmar si se definen un proceso o un marco para el desarrollo, revisión y ajuste de una actuación y un plan de capacidad.
- Infórmese a través de entrevistas con miembros clave del personal involucrado en el desarrollo del plan de desempeño y la capacidad de si los elementos adecuados (por ejemplo, el clientenecesidades, los requerimientos del negocio, el costo, los requisitos de rendimiento de las aplicaciones, los requisitos de escalabilidad) han sido considerados durante el desarrollo de lacapacidad del plan.

- Averiguar y confirmar si el plan de desempeño y la capacidad se han desarrollado y se mantiene.
- Inspeccione los documentos justificativos para comprobar la participación de los interesados y para asegurar que el plan se ha registrado y está al día.

DS3.2 Capacidad y Desempeño Actual

Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidady desempeño para prestar los servicios con base en los niveles de servicio acordados.

10.3.1 Gestión de la capacidad

Control

Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones delos requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

Guía de implementación

Para cada actividad nueva y existente es conveniente identificar los requisitos de la capacidad.Se recomienda monitorear y adaptar el sistema para garantizar y, cuando sea necesario,mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles deindagación para indicar los problemas en el momento oportuno. En las proyecciones de losrequisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos delsistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento deinformación de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requierecostos elevados; por lo tanto, los directores deberían monitorear la utilización de los recursosclaves del sistema. También deberían identificar las tendencias del uso, particularmente enrelación con las aplicaciones del negocio o las herramientas del sistema de información para lagestión.

Es conveniente que los directores utilicen esta información para identificar y evitar posiblescuellos de botella así como la dependencia de personal clave, los cuales pueden presentar unaamenaza para los servicios o la seguridad del sistema, y para planificar la acción adecuada.

DS3.3 Capacidad y Desempeño Futuros

Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo deinterrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso decapacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que seránparte de los planes de capacidad y de desempeño.

10.3.1 Gestión de la capacidad

Control

Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones delos requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

Guía de implementación

Para cada actividad nueva y existente es conveniente identificar los requisitos de la capacidad.Se recomienda monitorear y adaptar el sistema para garantizar y, cuando sea necesario,mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles deindagación para indicar los problemas en el momento oportuno. En las proyecciones de losrequisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos delsistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento deinformación de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requierecostos elevados; por lo tanto, los directores deberían monitorear la utilización de los recursosclaves del sistema. También deberían identificar las tendencias del uso, particularmente enrelación con las aplicaciones del negocio o las herramientas del sistema de información para lagestión.

Es conveniente que los directores utilicen esta información para identificar y evitar posiblescuellos de botella así como la dependencia de personal clave, los cuales pueden presentar unaamenaza para los servicios o la seguridad del sistema, y para planificar la acción adecuada.

Guías de Aseguramiento

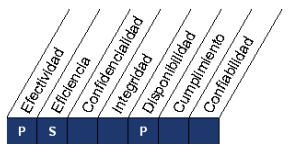
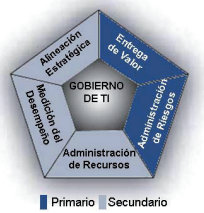
- Averiguar y confirmar si el software de monitorización del sistema se ha aplicado en el caso los recursos de TI basados en factores tales como:
  - Empresas de la criticidad de los recursos de TI.
  - Requerimientos identificados en el SLA.
  - Riesgo o la tendencia histórica de los recursos de TI a tener problemas de rendimiento o de capacidad.
  - Operacionales, financieras y de impacto regulatorio de los problemas de rendimiento o de capacidad.
- Determinar si los umbrales se han establecido y aplicado en los recursos de TI basada en los requerimientos del negocio y los SLAs. Ejemplos de umbrales son:
  - El centro de llamadas de añadir capacidad en las líneas troncales adicionales sin costo de entrada cuando los troncos son el 80 por ciento de ocupados.
  - Servidores de añadir el espacio de disco adicional cuando los discos duros alcanzar un nivel de capacidad específica.
- Determinar cómo los incidentes de ejecución deficiente son identificados y rastreados.
- Obtención de tickets y rastrear transacciones identificadas a través del sistema para determinar si un seguimiento adecuado se ha producido.

- Infórmese de los miembros clave del personal responsable de la entrega de la organización con los SLA para determinar cómo monitorear, rastrear e informar sobre la capacidad de recursos de TI ymétricas de rendimiento.

- Revisar los informes operacionales que se proporcionan a los principales interesados.

DS4 Garantizar la Continuidad del Servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI,almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo decontinuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones yprocesos claves del negocio.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS4.1 Marco de Trabajo de Continuidad de TI

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largode toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de lainfraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.

El marco de trabajo debe tomaren cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de losproveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar,probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales comola identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y losprincipios de respaldo y recuperación.

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

6.1.7 Contactos con grupos de interés especiales

Control

Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

Guía de implementación

La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.

b) garantizar que la comprensión del entorno de seguridad de la información es actual y completa.

c) recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.

d) obtener acceso a asesoría especializada sobre seguridad de la información.

e) compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

f) suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

14.1.4 Estructura para la planificación de la continuidad del negocio

Control

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.

Guía de implementación

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan. Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un dueño específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de seguridad de la información identificados y considera los siguientes aspectos:

a) Las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.

b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.

c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.

d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.

e) Los procedimientos de reanudación que describen las acciones por realizar para que lasoperaciones del negocio vuelvan a la normalidad.

f) Una programación de mantenimiento que especifique cómo y cuándo se realizaránpruebas al plan y el proceso para el mantenimiento del plan.

g) Actividades de concientización, educación y formación diseñadas para comprender losprocesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.

h) Las responsabilidades de las personas, que describan quién es responsable de laejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.

i) Los activos y recursos críticos necesarios para ejecutar los procedimientos deemergencia, respaldo y reanudación.

Guías de Aseguramiento

- Averiguar y confirmar si un proceso de gestión de la continuidad de negocio en toda la empresa está diseñado y aprobado por la administración a nivel ejecutivo.

- Inspeccione el análisis de impacto sobre las empresas actuales y determinar si la planificación de la continuidad se ha traducido en posicionamiento claro de los recursos necesarios para recuperar el negocio las operaciones durante una interrupción.

- Inspeccione el marco de la continuidad del negocio para confirmar que incluye todos los elementos necesarios para reanudar el proceso de negocio en el caso de una interrupción del negocio (Considerar la rendición de cuentas, la comunicación, el plan de escalada, las estrategias de recuperación, de TI y los niveles de negocio de servicios y procedimientos de emergencia).

DS4.2 Planes de Continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayorde las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamientoalternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles yresponsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

6.1.7 Contactos con grupos de interés especiales

Control

Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

Guía de implementación

La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.

b) garantizar que la comprensión del entorno de seguridad de la información es actual y completa.

c) recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.

d) obtener acceso a asesoría especializada sobre seguridad de la información.

e) compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

f) suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Control

Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones yasegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos,después de la interrupción o la falla de los procesos críticos para el negocio.

Guía de implementación

En el proceso de planificación de la continuidad del negocio se deberían considerar lossiguientes aspectos:

a) Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio.

b) Identificar la pérdida aceptable de información y servicios.

c) Implementar los procedimientos que permitan recuperar y restaurar las operaciones delnegocio y la disponibilidad de la información en las escalas de tiempo requeridas; esnecesario atender la evaluación de las dependencias internas y externas del negocio y de los contratos establecidos.

d) Procedimientos operativos que se han de seguir en espera de la terminación de larecuperación y restauración.

e) Documentación de procedimientos y procesos acordados.

f) Formación apropiada del personal en los procedimientos y procesos acordados,incluyendo el manejo de las crisis.

g) Pruebas y actualización de los planes:

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, porejemplo la restauración de servicios de comunicación específicos para los clientes en un lapsode tiempo aceptable.

Los servicios y recursos que lo facilitan deberían identificarse, incluyendoel personal, los recursos no relacionados con el procesamiento de información, al igual que lasdisposiciones de respaldo para los servicios de procesamiento de información. Estasdisposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdosrecíprocos o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organizacióny, por lo tanto, pueden contener información sensible que es necesario protegeradecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenaren un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre enla sede principal. La dirección debería garantizar que las copias de los planes de continuidaddel negocio están actualizadas y protegidas con el mismo nivel de seguridad que se aplica enla sede principal. De igual modo, el otro material necesario para ejecutar los planes decontinuidad se debería almacenar en un sitio lejano.

Si se utilizan lugares alternos temporales, el nivel de los controles de seguridad implementadosen estos lugares debería ser equivalente al de la sede principal.

Guías de Aseguramiento

- Confirme que los planes de continuidad de negocio existen para todas las funciones clave de negocio y procesos.
- Revisión de una muestra adecuada de los planes de continuidad del negocio y confirmar que cada plan:
  - Está diseñado para establecer la capacidad de recuperación, el tratamiento alternativo y la capacidad de recuperación, de conformidad con los compromisos de servicio y objetivos de disponibilidad.

- Define las funciones y responsabilidades.
- Incluye los procesos de comunicación.
- Define la configuración mínima aceptable de recuperación.

- Obtener la estrategia de ensayo general para los planes de continuidad del negocio y las pruebas que las pruebas se ejecutan con la frecuencia acordada.
- Revisar los resultados de las pruebas, y asegurar que las acciones resultantes son objeto de seguimiento.

DS4.3 Recursos Críticos de TI

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia yestablecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse deque la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que loscostos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar losrequerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, decuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

Guías de Aseguramiento

- Obtener una lista de funciones de negocios con su carácter crítico de negocio correspondiente, y asegurarse de que existen planes de continuidad de las funciones de negocio más críticos, el apoyo a procesos y recursos.
- Revisar los planes para asegurarse de que se han diseñado (y probado) para cumplir con los objetivos de negocio y los requisitos legales y reglamentarios.
- Determinar cómo la coherencia entre los planes está garantizada.

DS4.4 Mantenimiento del Plan de Continuidad de TI

Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TIse mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios enlos procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal

b) Las direcciones o los números telefónicos

c) La estrategia del negocio

d) Los lugares, dispositivos y recursos

e) La legislación

f) Los contratistas, proveedores y clientes principales

g) Los procesos existentes, nuevos o retirados

h) Los riesgos(operativos y financieros)

Guías de Aseguramiento

- Averiguar y confirme si todas las copias del plan de continuidad de TI estén actualizados con las revisiones y se almacenan en línea y fuera de las instalaciones.
- Averiguar y confirmar si todos los cambios fundamentales para los recursos de TI se comunican al gerente de la continuidad para la actualización del plan de continuidad de la TI.
- Averiguar y confirmar si los cambios en el plan de continuidad se realicen a intervalos adecuados para los factores desencadenantes y seguir los procedimientos aceptados de control de cambios.

DS4.5 Pruebas del Plan de Continuidad de TI

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva,que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación,reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar elalcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta apunta y en pruebas integradas con el proveedor.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal

b) Las direcciones o los números telefónicos

c) La estrategia del negocio

d) Los lugares, dispositivos y recursos

e) La legislación

f) Los contratistas, proveedores y clientes principales

g) Los procesos existentes, nuevos o retirados

h) Los riesgos(operativos y financieros)

Guías de Aseguramiento

- Averiguar y confirmar si las pruebas de continuidad son regulares y terminó de forma regular después de los cambios en la infraestructura de TI o de negocios y afines con las aplicaciones.

- Asegúrese de que los nuevos componentes y actualizaciones están incluidos en el calendario.

- Averiguar y confirmar si un calendario detallado de las pruebas se ha creado, e incluye detalles de las pruebas y la cronología de eventos para garantizar una secuencia lógica y real de se producen interrupciones.

- Averiguar y confirmar si un grupo de trabajo de ensayo se ha establecido, y los miembros no sean personal básico definido en el plan y la presentación de informes es el adecuado.

- Infórmese a través de entrevistas con miembros clave del personal si los eventos que ocurren son informativos y, dentro de estos eventos, si se analizan las fallas y soluciones desarrolladas.

- Infórmese a través de entrevistas con miembros clave del personal si los medios alternativos se evalúan en las pruebas no es factible.

- Averiguar y confirmar si el éxito o el fracaso de la prueba se mide y se informa y el consiguiente cambio se hace para el plan de continuidad de TI.

- Revisar los resultados y evaluar los resultados se revisan para determinar la eficacia de funcionamiento.

DS4.6 Entrenamiento del Plan de Continuidad de TI

Asegurarse de que todos las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus rolesy responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de laspruebas de contingencia.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal

b) Las direcciones o los números telefónicos

c) La estrategia del negocio

d) Los lugares, dispositivos y recursos

e) La legislación

f) Los contratistas, proveedores y clientes principales

g) Los procesos existentes, nuevos o retirados

h) Los riesgos(operativos y financieros)

Guías de Aseguramiento

- Infórmese a través de entrevistas con miembros clave de si el entrenamiento se realiza regularmente.
- Averiguar y confirmar si las necesidades de formación y programas son evaluadas y actualizadas regularmente.
- Revisión de programas y material de capacitación para determinar la efectividad operativa.
- Infórmese a través de entrevistas con miembros clave del personal si la continuidad de los programas de sensibilización se llevan a cabo en todos los niveles.

DS4.7 Distribución del Plan de Continuidad de TI

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de maneraapropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestaratención en hacerlos accesibles bajo cualquier escenario de desastre.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal

b) Las direcciones o los números telefónicos

c) La estrategia del negocio

d) Los lugares, dispositivos y recursos

e) La legislación

f) Los contratistas, proveedores y clientes principales

g) Los procesos existentes, nuevos o retirados

h) Los riesgos(operativos y financieros)

Guías de Aseguramiento

- Averiguar y confirmar si una lista de distribución para el plan de continuidad de la TI se ha creado, definido y mantenido. Revisar si la necesidad de conocer los principios han sido mantenido durante el desarrollo de la lista.
- Obtener el procedimiento de distribución de la gestión.
- Evaluar el procedimiento y verificar su cumplimiento.
- Averiguar y confirme si todas las copias digitales y físicas del plan están protegidos de manera adecuada y que los documentos son accesibles únicamente por personal autorizado.

DS4.8 Recuperación y Reanudación de los Servicios de TI

Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar laactivación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizarprocedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI ylas inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Control

Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones yasegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos,después de la interrupción o la falla de los procesos críticos para el negocio.

Guía de implementación

En el proceso de planificación de la continuidad del negocio se deberían considerar lossiguientes aspectos:

a) Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio.

b) Identificar la pérdida aceptable de información y servicios.

c) Implementar los procedimientos que permitan recuperar y restaurar las operaciones delnegocio y la disponibilidad de la información en las escalas de tiempo requeridas; esnecesario atender la evaluación de las dependencias internas y externas del negocio y de los contratos establecidos.

d) Procedimientos operativos que se han de seguir en espera de la terminación de larecuperación y restauración.

e) Documentación de procedimientos y procesos acordados.

f) Formación apropiada del personal en los procedimientos y procesos acordados,incluyendo el manejo de las crisis.

g) Pruebas y actualización de los planes:

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, porejemplo la restauración de servicios de comunicación específicos para los clientes en un lapsode tiempo aceptable. Los servicios y recursos que lo facilitan deberían identificarse, incluyendoel personal, los recursos no relacionados con el procesamiento de información, al igual que lasdisposiciones de respaldo para los servicios de procesamiento de información. Estasdisposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdosrecíprocos o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organizacióny, por lo tanto, pueden contener información sensible que es necesario protegeradecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenaren un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre enla sede principal. La dirección debería garantizar que las copias de los planes de continuidaddel negocio están actualizadas y protegidas con el mismo nivel de seguridad que se aplica enla sede principal. De igual modo, el otro material necesario para ejecutar los planes decontinuidad se debería almacenar en un sitio lejano.

Si se utilizan lugares alternos temporales, el nivel de los controles de seguridad implementadosen estos lugares debería ser equivalente al de la sede principal.

Guías de Aseguramiento

- Obtener una copia del procedimiento de gestión de incidentes, y asegurar que incluye los pasos para la evaluación de daños, así como los puntos formales de decisión y umbrales para activarplanes de continuidad.
- Revisión de los planes de recuperación de TI, y comprobar que cumplen con los requerimientos del negocio.

DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para larecuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse enconjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamientoexterno a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de laempresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez poraño, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del softwarepara poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

10.5.1 Respaldo de la información

Control

Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

Guía de implementación

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información: Es recomendable definir el nivel necesario para la información de respaldo.

a) Es recomendable definir el nivel necesario para la información de respaldo.

b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la organización.

d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.

e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental (véase el numeral 9) consistente con las normas aplicadas en la sede principal; los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo.

f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.

g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación.

h) En situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el periodo de retención de la información esencial para el negocio, asícomo cualquier requisito para retener permanentemente las copias de archivo.

Guías de Aseguramiento

- Averiguar y confirmar si los datos están protegidos cuando se toman fuera de las instalaciones, mientras están en el transporte y cuando están en el lugar de almacenamiento.
- Averiguar y confirmar si las instalaciones de respaldo no están sujetos a los mismos riesgos que el sitio primario.
- Averiguar y confirmar si la prueba regular se realiza para garantizar la calidad de las copias de seguridad y los medios de comunicación.
- Revisión de los procedimientos de prueba para determinar la efectividad operativa.
- Verificar que los medios de copia de seguridad contiene toda la información requerida por el plan de continuidad de la TI, por ejemplo, al comparar el contenido de las copias de seguridad y / o restaurar los sistemas con los sistemas operativos.
- Averiguar y confirmar si las instrucciones de recuperación suficiente y etiquetado de existir.
- Averiguar y confirmar si un inventario de las copias de seguridad y los medios de comunicación existe, y verificar su exactitud.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS4.10 Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI haestablecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

14.1.5 Pruebas, mantenimiento y evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio debería asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son consientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, conocer su función cuando se ejecuta un plan.

La programación para las pruebas para los planes de continuidad del negocio deberían indicar cómo y cuándo se va aprobar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionaran en condiciones reales. Estas incluirán:

a) La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplo de interrupciones).

b) Las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes).

c) Las pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente).

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal).

e) Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).

f) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se debería registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidades para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se refleja en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplo de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, mejora de los sistemas y cambios en:

a) El personal

b) Las direcciones o los números telefónicos

c) La estrategia del negocio

d) Los lugares, dispositivos y recursos

e) La legislación

f) Los contratistas, proveedores y clientes principales

g) Los procesos existentes, nuevos o retirados

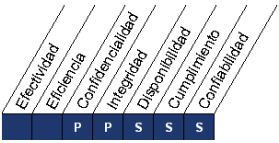
h) Los riesgos(operativos y financieros)

Guías de Aseguramiento

- Averiguar y confirmar si las deficiencias del plan se han destacado y reuniones de la recuperación después de discutir las oportunidades de mejora se llevan a cabo.
- Revisar los planes, políticas y procedimientos para determinar la efectividad operativa.

DS5 Garantizar la Seguridad de los Sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración dela seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas,estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebasperiódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectivaadministración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades oincidentes de seguridad.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS5.1 Administración de la Seguridad de TI

Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración dela seguridad estén en línea con los requerimientos del negocio.

6.1.1 Compromiso de la dirección con la seguridad de la información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guías de implementación

la dirección debería:

a) Asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.

b) Formular, revisar y aprobar la política de seguridad de la información.

c) Revisar la eficacia de la implementación de la política de seguridad de la información.

d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.

e) Proporcionar los recursos necesarios para la seguridad de la información.

f) Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización.

g) Iniciar planes y programas para mantener la concientización sobre la seguridad de la información.

h) Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor a través de un organismo de dirección ya existente, como por ejemplo el concejo directivo.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

   4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

   5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

   6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

   7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

   1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

   2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

   3) Proceso de autorización para los privilegios y el acceso de usuario.

   4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

   5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

   6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Determinar si un comité de dirección de seguridad existe, con representación de las principales áreas funcionales, incluida la auditoría interna, recursos humanos, operaciones, seguridad informática y jurídica.

- Determinar si existe un proceso para dar prioridad a las iniciativas propuestas de seguridad, incluyendo los niveles requeridos de las políticas, normas y procedimientos.

- Averiguar y confirmar si una carta de seguridad de la información existe.

- Revisar y analizar la carta para verificar que se refiere al apetito por el riesgo de organización relativos a la seguridad de la información y que la carta contiene de manera clara:

  - Ámbito de aplicación y objetivos de la función de gestión de la seguridad.

  - Responsabilidades de la función de gestión de la seguridad.

  - Cumplimiento de los conductores y el riesgo.

- Averiguar y confirmar si la política de seguridad de la información cubre las responsabilidades del consejo de administración, dirección ejecutiva, la gestión de la línea, los funcionarios y todos losusuarios de la empresa de infraestructura de TI y que se refiere a las normas de seguridad y procedimientos detallados.

- Pregunte y confirmesi, una política de seguridad detallada, las normas y procedimientos existen ejemplos de políticas, normas y procedimientos incluyen:

- Política de seguridad de cumplimiento.
- Gestión de aceptación del riesgo (seguridad reconocimiento incumplimiento).
- Comunicaciones externas política de seguridad.
- La política de firewall.
- E-mail política de seguridad.
- Un acuerdo para cumplir con las políticas de IS.
- Ordenador portátil / ordenador de sobremesa política de seguridad.
- Política de uso de Internet.

- Averiguar y confirmar si, una estructura organizacional adecuada y la línea de información para seguridad de la información existentes, y evaluar si la gestión de la seguridad yfunciones de administración tienen la autoridad suficiente.
- Averiguar y confirmar si un mecanismo de gestión de la seguridad de información que existe informa la Junta, las empresas y la administración de TI de la situación deseguridad de la información.

DS5.2 Plan de Seguridad de TI

Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo enconsideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas yprocedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar laspolíticas y procedimientos de seguridad a los interesados y a los usuarios.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

incluyendo los siguientes:

1) cumplimiento de los requisitos legales, reglamentarios y contractuales;

2) requisitos de educación, formación y concientización sobre seguridad;

3) gestión de la continuidad del negocio;

4) consecuencias de las violaciones de la política de seguridad;

e) definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como “necesidad de conocer”).

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

11.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) requisitos de seguridad de las aplicaciones individuales del negocio.

b) identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.

c) políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información.

d) consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.

e) legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.

f) perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.

g) gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.

h) distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.

i) requisitos para la autorización formal de las solicitudes de acceso.

j) requisitos para la revisión periódica de los controles de acceso.

k) retiro de los derechos de acceso.

11.7.1 Computación y comunicaciones móviles

Control

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Guía de implementación

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (*notebooks*), microcomputadores de bolsillo (*palmtops*), y computadores portátiles pesados (*laptops*), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos sin protección.

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio. Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información. Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes debería tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y / o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

11.7.2 Trabajo remoto

Control

Se debería desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guías de implementación

Las organizaciones solo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) Seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.

b) El entorno físico de trabajo remoto propuesto.

c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el alcance de comunicación y la sensibilidad del sistema interno.

d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio por ejemplo familiares y amigos.

e) El uso de redes domesticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.

f) Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.

g) El acceso al equipo de propiedad (para verificar la seguridad de la maquina o durante una investigación), el cual puede estar prohibido por la ley.

h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

i) Protección de antivirus y requisitos de firewall.

Las directrices y disposiciones a considerar debería incluir las siguientes:

a) Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.

b) Definición del trabajo que se permite realizar, las horas laborales, la confidencialidad de la información que se conserva y los sistemas y los servicios internos para los cuales el trabajador tiene acceso autorizado.

c) Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.

d) Seguridad física.

e) Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

f) Disposición de soporte y mantenimiento de hardware y software.

g) Disposición de pólizas de seguros.

h) Procedimientos para el respaldo y la continuidad del negocio.

i) Auditoria y monitoreo de seguridad.

j) Revocación de auditoría y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

Guías de Aseguramiento

- Determinar la eficacia de la recolección e integración de los requisitos de seguridad de la información en un plan general de seguridad de TI que responda a las necesidades cambiantes de la organización.

- Verifique que el plan de seguridad que lo considere planes tácticos (PO1), clasificación de datos (PO2), los estándares de tecnología (PO3), la seguridad y las políticas de control (PO6), el riesgo gestión (PO9), y el cumplimiento de los requisitos externos (ME3).

- Determinar si existe un proceso para actualizar periódicamente el plan de seguridad de TI, y si el proceso requiere de niveles adecuados de examen de la gestión y aprobación de los cambios.
- Determinar si la empresa las líneas de base de seguridad de información para todas las plataformas principales son acordes con el plan general de seguridad de TI, si las líneas de base se han registrado en la línea de base de configuración (DS9) repositorio central, y si existe un proceso para actualizar periódicamente las líneas de base sobre la base de los cambios en el plan.
- Determinar si el plan de seguridad de TI incluye lo siguiente:
  - Un juego completo de las políticas y normas de seguridad en línea con el marco de la política de información establecida de seguridad.
  - Los procedimientos para aplicar y hacer cumplir las políticas y normas.
  - Funciones y responsabilidades.
  - Necesidades de personal.
  - Sensibilización y formación.
  - Aplicación de las prácticas.
  - Las inversiones en recursos de seguridad necesarios.
- Determinar si existe un proceso para integrar las exigencias de seguridad de la información y asesoramiento sobre la ejecución del plan de seguridad de TI en otros procesos, incluido eldesarrollo de los SLA y OLA (DS1-DS2), los requisitos de solución automatizada (AI1), software de aplicación (AI2), y componentes de la infraestructura de TI (AI3).

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS5.3 Administración de Identidad

Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno deTI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario seidentifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos estánen línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a lasidentidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por elresponsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos deacceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienenactualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

incluyendo los siguientes:

1) cumplimiento de los requisitos legales, reglamentarios y contractuales;

2) requisitos de educación, formación y concientización sobre seguridad;

3) gestión de la continuidad del negocio;

4) consecuencias de las violaciones de la política de seguridad;

e) definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representante de todas las partes de la organización con roles y funciones laborales pertinentes.

Guías de implementación

Comúnmente la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgo.

Esta actividad debería:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de seguridad de la información.

b) Identificar la forma de manejar los incumplimientos.

c) Aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de la información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.

f) Promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización.

g) Valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea grupos con funciones separadas, por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otros organismos de la dirección o un solo director.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

11.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) requisitos de seguridad de las aplicaciones individuales del negocio.

b) identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.

c) políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información.

d) consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.

e) legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.

f) perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.

g) gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.

h) distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.

i) requisitos para la autorización formal de las solicitudes de acceso.

j) requisitos para la revisión periódica de los controles de acceso.

k) retiro de los derechos de acceso.

11.7.1 Computación y comunicaciones móviles

Control

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Guía de implementación

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (*notebooks*), microcomputadores de bolsillo (*palmtops*), y computadores portátiles pesados (*laptops*), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos sin protección.

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio. Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información. Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes debería tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y / o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

11.7.2 Trabajo remoto

Control

Se debería desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guías de implementación

Las organizaciones solo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) Seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.

b) El entorno físico de trabajo remoto propuesto.

c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el alcance de comunicación y la sensibilidad del sistema interno.

d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio por ejemplo familiares y amigos.

e) El uso de redes domesticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.

f) Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.

g) El acceso al equipo de propiedad (para verificar la seguridad de la maquina o durante una investigación), el cual puede estar prohibido por la ley.

h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

i) Protección de antivirus y requisitos de firewall.

Las directrices y disposiciones a considerar debería incluir las siguientes:

a) Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.

b) Definición del trabajo que se permite realizar, las horas laborales, la confidencialidad de la información que se conserva y los sistemas y los servicios internos para los cuales el trabajador tiene acceso autorizado.

c) Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.

d) Seguridad física.

e) Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

f) Disposición de soporte y mantenimiento de hardware y software.

g) Disposición de pólizas de seguros.

h) Procedimientos para el respaldo y la continuidad del negocio.

i) Auditoria y monitoreo de seguridad.

j) Revocación de auditoría y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

Guías de Aseguramiento

- Determinar si las prácticas de seguridad requieren que los usuarios y los procesos del sistema de identificación de forma inequívoca y sistemas para ser configurado para aplicar la autenticación antes de que el acceso es concedido.

- Si los roles predeterminados y aprobación previa se utilizan para permitir el acceso, determinar si las funciones claramente las responsabilidades sobre la base de privilegios mínimos y garantizar que el establecimiento y modificación de los roles son aprobados por la gestión de procesos propietario.

- Determinar si el acceso de aprovisionamiento y mecanismos de autenticación de control se utilizan para el control de acceso lógico a través de todos los usuarios, los procesos del sistema y los recursos de TI, ya que en la casa y gestión remota de los procesos de usuarios y sistemas.

DS5.4 Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegiosrelacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse unprocedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estosprocedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos einternos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de laempresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas lascuentas y los privilegios asociados.

6.1.5 Acuerdos sobre confidencialidad

Control

Se debería identifica y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que refleja las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se pueden hacer cumplir legalmente. Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) Definición de la información que se protege (por ejemplo información confidencial).

b) Duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad definidamente.

c) Acciones requeridas cuando se termina un acuerdo.

d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer").

e) Propiedad de la información, secretos comerciales, propiedad intelectual y como se relaciona con la protección de la información confidencial.

f) El uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información.

g) Derecho de auditar y monitorear las actividades que involucran a la información confidencial.

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial.

i) Términos para la devolución o destrucción de la información al terminar el acuerdo.

j) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de no confidencialidad o no- divulgación.

Los acuerdos de confidencialidad o no- divulgación deberían cumplir todas las leyes y las regulaciones que se aplican que se aplican en la jurisdicción correspondiente.

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan es estos requisitos.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

   1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

   2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

   3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

   4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

6.2.2 Abordaje de la seguridad cuando se trata con los clientes

Control

Todos los requisitos de seguridad identificados se deberían abordar antes de dar acceso a los clientes a los activos o la información de la organización.

Guía de implementación

Los siguientes términos se deberían considerar para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización (dependiendo del tipo y la extensión de dicho acceso, no se podrían aplicar todos ellos):

a) protección de activos, incluyendo:

   1) procedimientos para proteger los activos de la organización, incluyendo información y software, y gestión de las vulnerabilidades conocidas.

   2) procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de datos.

   3) Integridad.

   4) restricciones a la copia y la divulgación de la información.

b) descripción del producto o servicio que se va proveer.

c) las diversas razones, requisitos y beneficios del acceso del cliente.

d) política de control del acceso, incluyendo:

1) métodos de acceso permitido y control y uso de identificadores únicos tales como la identificación del usuario (ID) y las contraseñas.

2) proceso de autorización para los privilegios y el acceso de los usuarios.

3) declaración de que el acceso que no se autorice explícitamente está prohibido.

4) proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

e) convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de detalles personales), incidentes de seguridad de la información y violaciones de la seguridad.

f) descripción de cada servicio que va a estar disponible.

g) la meta del nivel de servicio y los niveles inaceptables de servicio.

h) el derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

i) las respectivas responsabilidades civiles de la organización y del cliente.

j) las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con clientes en otros países.

k) derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.

8.1.1 Roles y responsabilidades

Control

Se deberían definir y documentar los roles y las responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo de acuerdo con las políticas de seguridad de la información de la organización.

b) Proteger los activos contra accesos, divulgación, modificación, destrucción o interferencia no autorizados.

c) Ejecutar proceso o actividades particulares de seguridad.

d) Garantiza que se asigna la responsabilidad a la persona para que tome las acciones.

e) Informar los eventos de seguridad, los eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones y responsabilidades de seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

8.3.1 Responsabilidades en la terminación

Control

Se deberían definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.

Guía de implementación

La comunicación de las responsabilidades en la terminación debería incluir los requisitos permanentes de seguridad y las responsabilidades legales y, cuando sea apropiado, las responsabilidades contenidas en cualquier acuerdo de confidencialidad y los términos y condiciones laborales deberían continuar durante un periodo definido después de terminar la contratación laboral del empleado, el contratista o el usuario de terceras partes.

Los contratos del empleado, el contratista o el usuario de terceras partes deberían incluir las responsabilidades y deberes válidos aún después de la terminación del contrato laboral.

Los cambios en la responsabilidad o en el contrato laboral deberían ser gestionados como la terminación de la responsabilidad o el contrato laboral respectivo, y la nueva responsabilidad o contrato laboral se debería controlar tal como se describe en el numeral 8.1.

8.3.3 Retiro de los derechos de acceso

Control

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deberían retirar al finalizar su contratación laboral, contrato o acuerdo o se deberían ajustar después del cambio.

Guía de implementación

Después de la terminación, se deberían reconsiderar los derechos de acceso de la persona a los activos asociados con los sistemas y servicios de información. Ello determinará si es necesario retirar los derechos de acceso. Los cambios en un cargo se deberían reflejar en el retiro de todos los derechos de acceso que no estén aprobados para el nuevo cargo.

Los derechos de acceso que se deberían adaptar o retirar incluyen acceso físico y lógico, claves, tarjetas de identificación, servicios de procesamiento de información, suscripciones y retiro de cualquier documentación que lo identifique como miembro actual de la organización. Si un empleado, contratista o usuario de terceras partes que se retira tiene contraseñas conocidas para permanecer activo, éstas se deberían cambiar en la terminación o el cambio de empleo, contrato o acuerdo.

Los derechos de acceso a los activos de información y a los servicios de procesamiento de información se deberían reducir o retirar antes de la finalización o cambio del contrato laboral, dependiendo de la evaluación de factores de riesgo tales como:

a) si la terminación o el cambio es iniciativa del empleado, contratista o usuario de terceras partes o por la dirección y el motivo de dicha terminación.

b) las responsabilidades actuales del empleado, contratista o cualquier otro usuario.

c) el valor de los activos actualmente accesibles.

10.1.3 Distribución (Segregación) de funciones

Control

Las funciones y las áreas de responsabilidad se deberían distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

Guías de implementación

La distribución de funciones es un método para reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se debería tener cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento se debería separar de su autorización. Es conveniente considerar la posibilidad de complicidad al diseñar los controles.

Las organizaciones pequeñas pueden encontrar difícil de lograr la distribución de funciones, pero el principio se debería aplicar en la medida de lo posible y viable. Siempre que haya dificultad para la distribución, se deberían considerar otros controles como monitoreo de actividades, registros de auditoría y supervisión por la dirección. Es importante que la auditoria de seguridad siga siendo independiente.

11.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) requisitos de seguridad de las aplicaciones individuales del negocio.

b) identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.

c) políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información.

d) consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.

e) legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.

f) perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.

g) gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.

h) distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.

i) requisitos para la autorización formal de las solicitudes de acceso.

j) requisitos para la revisión periódica de los controles de acceso.

k) retiro de los derechos de acceso.

11.2.1 Registro de usuarios

Control

Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin deconceder y revocar el acceso a todos los sistemas y servicios de información.

Guía de implementación

El procedimiento de control del acceso para el registro y cancelación de usuarios deberíaincluir:

a) Uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o del negocio, y deberían estar aprobados y documentados.

b) Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección apruebe por separado los derechos de acceso.

c) Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos del negocio y sea consistente con la política de seguridad de la organización, es decir, no pone en peligro la distribución de funciones.

d) Dar a los usuarios una declaración escrita de sus derechos de acceso.

e) Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.

f) Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.

g) Mantenimiento de un registro formal de todas las personas registradas para usar el servicio.

h) Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.

i) Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios.

j) Garantizar que las identificaciones (ID) de usuario redundantes no se otorgan a otros usuarios.

11.2.2 Gestión de privilegios

Control

Se debería restringir y controlar la asignación y el uso de privilegios.

Guía de implementación

Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían controlar la asignación de privilegios a través de un proceso formal de autorización.

Se recomienda tener en cuenta los siguientes elementos:

a) Se deberían identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y aplicaciones.

b) Se deberían asignar los privilegios a los usuarios sobre los principios de necesidad-deuso y evento-por-evento, y de manera acorde con la política de control de acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario.

c) se deberían conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo.

d) es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

e) se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.

f) los privilegios se deberían asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio.

11.2.4 Revisión de los derechos de acceso de los usuarios

Control

La dirección debería establecer un procedimiento formal de revisión periódica de los derechosde acceso de los usuarios.

Guía de implementación

Se recomienda que en la revisión de los derechos de acceso se consideren las siguientesdirectrices:

a) Los derechos de acceso de los usuarios se deberían revisar a intervalos regulares, por ejemplo cada seis meses y después de cada cambio, como por ejemplo promoción, cambio a un cargo en un nivel inferior, o terminación del contrato laboral.

b) Los derechos de acceso de usuarios se debería revisar y reasignar cuando hay cambios de un cargo a otro dentro de la misma organización.

c) Es recomendable revisar las autorizaciones para derechos de acceso privilegiado a intervalos más frecuentes, por ejemplo cada tres meses.

d) Se debería verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.

e) Los cambios en las cuentas privilegiadas se deberían registrar para su revisión periódica.

11.3.1 Uso de contraseñas

Control

Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

Guía de implementación

Todos los usuarios deberían:

a) mantener la confidencialidad de las contraseñas;

b) evitar conservar registros (por ejemplo en papel, archivos de software o dispositivos manuales) de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

c) cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña;

d) seleccionar contraseñas de calidad con longitud mínima suficiente que:

   1) sean fáciles de recordar;

   2) no se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.

   3) no sean vulnerables al ataque de diccionarios (es decir, que no consistan en palabras incluidas en diccionarios).

   4) no tengan caracteres idénticos consecutivos, que no sean todos numéricos ni todos alfabéticos.

e) cambiar las contraseñas a intervalos regulares o con base en el número de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas.

f) cambiar las contraseñas temporales en el primer registro de inicio.

g) no incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.

h) no compartir las contraseñas de usuario individuales.

i) no utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que pueden usar una sola contraseña de calidad para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

11.5.1 Procedimientos de registro de inicio seguro

Control

El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.

Guía de implementación

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.

b) Mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados.

c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.

d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta.

e) Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar:

   1) Registrar intentos exitosos y fallidos.

   2) Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica.

   3) Desconectar las conexiones de enlaces de datos.

   4) Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio.

   5) Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege.

f) Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación;

g) Mostrar la siguiente información al terminar un registro de inicio exitoso:

   1) Fecha y hora del registro de inicio exitoso previo.

   2) Detalles de los intentos fallidos de registro de inicio desde el último registro exitoso.

h) No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos.

i) No transmitir contraseñas en texto claro en la red.

11.5.3 Sistema de gestión de contraseñas

Control

Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar lacalidad de las contraseñas.

Guía de implementación

Un sistema de gestión de contraseñas debería:

a) Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.

b) Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.

c) Imponer una elección de contraseñas de calidad.

d) Imponer cambios de contraseña.

e) Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio.

f) Conservar un registro de las contraseñas de usuario previas y evitar su reutilización.

g) No mostrar contraseñas en la pantalla cuando se hace su ingreso.

h) Almacenar los archivos de contraseñas separadamente de los datos del sistema de aplicación.

i) Almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo encriptadas o codificadas).

11.6.1 Restricción del acceso a la información

Control

Se debería restringir el acceso a la información y a las funciones del sistema de aplicación porparte de los usuarios y del personal de soporte, de acuerdo con la política definida de controlde acceso.

Guía de implementación

Las restricciones del acceso se deberían basar en los requisitos de las aplicacionesindividuales del negocio. La política de control de acceso también debería ser consistente conla política de acceso de la organización.

Se debería considerar la aplicación de las siguientes directrices con el objeto de dar soporte alos requisitos de restricción del acceso:

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.

b) Controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar.

c) Controlar los derechos de acceso de otras aplicaciones.

d) Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados; ello debería incluir revisiones periódicas de dichas salidas para garantizar el retiro de la información redundante.

Guías de Aseguramiento

- Determinar si existen procedimientos para evaluar y recertificar periódicamente el acceso al sistema y la aplicación y las autoridades.

- Determinar si los procedimientos de control de acceso existentes para controlar y gestionar los derechos de sistema y la aplicación y los privilegios de acuerdo a las políticas de seguridad de la organización y cumplimiento y los requisitos reglamentarios.

- Determinar si los sistemas, las aplicaciones y los datos han sido clasificados por niveles de importancia y riesgo, y si los dueños del proceso han sido identificados y asignados.
- Determinar si las políticas de aprovisionamiento de usuarios, normas y procedimientos se extienden a todos los usuarios del sistema y procesos, incluyendo vendedores, proveedores de servicios y socios de negocios.

DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe serreacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema(logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

10.10.2 Monitoreo del uso del sistema

Control

Se deberían establecer procedimientos para el monitoreo del uso de los servicios deprocesamiento de información, y los resultados de las actividades de monitoreo se deberíanrevisar con regularidad.

Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado, incluyendo detalles como:

   1) Identificación de usuario (ID).

   2) Fecha y hora de eventos clave.

3) Tipo de eventos.

4) Archivos a los que se ha tenido acceso.

5) Programas / utilidades empleados.

b) Todas las operaciones privilegiadas como:

1) Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.

2) Encendido y detención del sistema.

3) Acople / desacople del dispositivo de entrada / salida (I/O).

c) Intentos de acceso no autorizado, tales como:

1) Acciones de usuario fallidas o rechazadas.

2) Acciones fallidas o rechazadas que implican datos y otros recursos.

3) Violaciones de la política de acceso y notificaciones para las barreras de fuego (firewalls) y puertas de enlace (gateways).

4) Alertas de los sistemas de detección de intrusión de propietario.

d) Alertas o fallas del sistema como:

1) Alertas o mensajes de consola.

2) Excepciones de registro del sistema.

3) Alarmas de gestión de red.

4) Alarmas originadas por el sistema de control del acceso.

5) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.

b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.

d) Extensión de la interconexión del sistema (particularmente en redes públicas).

e) Servicio de operación de registro que se desactiva.

10.10.3 Protección de la información del registro

Control

Los servicios y la información de la actividad de registro se deberían proteger contra el accesoo la manipulación no autorizados.

Guía de implementación

Los controles deberían tener como objeto la protección contra cambios no autorizados yproblemas operativos con el servicio de registro incluyendo:

a) Alteraciones en los tipos de mensaje que se registran.

b) Archivos de registro que se editan o eliminan.

c) Capacidad de almacenamiento de los medios de archivo de registro que se exceden, lo que resulta en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

Puede ser necesario archivar algunos registros para auditoría como parte de la política deretención de registros o debido a los requisitos para recolectar y conservar evidencia.

10.10.4 Registros del administrador y del operador

Control

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

Guía de implementación

Los registros deberían incluir:

a) La hora en que ocurrió el evento (exitoso o fallido).

b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemploerrores que se presentaron y acciones correctivas que se tomaron).

c) Cuál cuenta y cuál administrador u operador estuvo involucrado.

d) Cuáles procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

   1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

   2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red.

   3) aumentar el monitoreo para detectar o prevenir los ataques reales.

   4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.

j) se deberían tratar primero los sistemas con alto riesgo.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

15.2.2 Verificación del cumplimiento técnico

Control

Los sistemas de información se deberían verificar periódicamente para determinar elcumplimiento con las normas de implementación de la seguridad.

Guía de implementación

La verificación del cumplimiento técnico se debería realizar bien sea manualmente (con soportede las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas conexperiencia y / o con la ayuda de herramientas automáticas que generan un informe técnicopara la interpretación posterior por parte del especialista técnico.

Si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tenercuidado puesto que dichas actividades pueden poner en peligro la seguridad del sistema. Talespruebas se deberían planificar, documentar y ser repetibles.

La verificación del cumplimiento técnico únicamente la deberían realizar personas autorizadas ycompetentes o bajo supervisión de dichas personas.

15.3.1 Controles de auditoría de los sistemas de información

Control

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

Guía de implementación

Se deberían tener presente las siguientes directrices:

a) los requisitos de auditoría se deberían acordar con la dirección correspondiente.

b) se debería acordar y controlar el alcance de las verificaciones.

c) las verificaciones se deberían limitar al acceso de sólo lectura del software y los datos.

d) el acceso diferente al de sólo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.

e) los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles.

f) se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.

g) todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar para datos o sistemas críticos.

h) se recomienda documentar todos los procedimientos, requisitos y responsabilidades.

i) la persona que realiza la auditoría debería ser independiente de las actividades auditadas.

Guías de Aseguramiento

- Averiguar y confirmar si un inventario de todos los dispositivos de red, servicios y aplicaciones existe y que cada componente se le ha asignado una calificación de riesgo de seguridad.

- Determinar si las bases de referencia de seguridad que existen para todas las TI utilizadas por la organización.

- Determinar si todos lo crítico la organización, los activos de red de alto riesgo se controla habitualmente para los eventos de seguridad.
- Determinar si la función de seguridad de TI de gestión se ha integrado dentro de las iniciativas de la organización de gestión de proyectos para garantizar que la seguridad se consideraendesarrollo, diseño y requisitos de prueba, para minimizar el riesgo de los sistemas nuevos o existentes, la introducción de las vulnerabilidades de seguridad.Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS5.6 Definición de Incidente de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificadospropiamente y tratados por el proceso de gestión de incidentes y problemas.

8.2.3 Proceso disciplinario

Control

Debería existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.

Guía de implementación

No se recomienda iniciar el proceso disciplinario antes de verificar que se ha presentado la violación de la seguridad.

El proceso disciplinario formal debería garantizar el tratamiento imparcial y correcto para los empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal debería brindar una respuesta gradual que considere factores tales como la naturaleza y la gravedad de la violación y su impacto en el negocio, si es la primera ofensa o se repite, si el violador está capacitado adecuadamente, la legislación correspondiente, los contratos de negocio y otros factores, según el caso. En los casos graves de mala conducta el proceso debería permitir el retiro instantáneo de las funciones, los derechos de acceso y los privilegios y el acompañamiento inmediato fuera de las instalaciones, si es necesario.

13.1.1 Reporte sobre los eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Guía de implementación

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empelados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema.

b) formatos para el reporte de los eventos de seguridad de la información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información.

c) el comportamiento correcto en caso de un evento de seguridad de la información, es decir:

    1) tomar nota inmediatamente sobre los detalles importantes (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño).

    2) no ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto.

d) referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de la seguridad.

En entornos de alto riesgo, se puede suministrar una alarma de coacción4) a través de la cual una persona bajo coacción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coacción deberían reflejar la situación de alto riesgo que indican tales alarmas.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

13.2.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Guía de implementación

Además del reporte de los eventos y las debilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades se debería emplear para detectar los incidentes de la seguridad de la información. Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de los incidentes de seguridad de la información:

a) es conveniente instaurar procedimientos para manejar los diferentes tipos de incidentes

de seguridad de la información, incluyendo:

1) fallas en el sistema de información y pérdida del servicio.
2) códigos maliciosos.
3) negación del servicio.
4) errores producidos por datos del negocio incompletos o inexactos.
5) violaciones de la confidencialidad y la integridad.
6) uso inadecuado de los sistemas de información.

b) además de los planes normales de contingencia, los procedimientos también deberían comprender:

   1) el análisis y la identificación de la causa del incidente.

   2) la contención.

   3) la planificación e implementación de la acción correctiva para evitar la recurrencia, si es necesario.

   4) la comunicación con aquellos afectados o implicados con la recuperación después del incidente.

   5) el reporte de la acción a la autoridad apropiada.

c) se deberían recolectar y asegurar los rastros para auditoría y la evidencia similar, según sea apropiado para:

   1) el análisis de los problemas internos;

   2) el uso de evidencia forense con respecto a la posible violación del contrato o del requisito reglamentario o en caso de juicios criminales o civiles, por ejemplo, según la legislación sobre uso inadecuado del computador o sobre protección de datos;

   3) la negociación para la compensación proveniente de los proveedores de software y servicios;

d) la acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada; los procedimientos deberían garantizar que:

   1) únicamente el personal claramente identificado y autorizado tiene acceso a los sistemas y datos activos.

   2) todas las acciones de emergencia están documentadas en detalle.

   3) la acción de emergencia se reporta a la dirección y se revisa de manera ordenada.

   4) la integridad de los sistemas y controles del negocio se confirma con retraso mínimo.

Los objetivos de la gestión de los incidentes de seguridad de la información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de seguridad de la información.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

Guías de Aseguramiento

- Determinar si un ComputerEmergency Response Team (CERT) existe para reconocer y gestionar eficazmente las emergencias de seguridad. Las siguientes áreas deben existir como parte de un efectivo proceso de CERT:

  - Manejo de Incidentes General y procedimientos específicos y otros requisitos para asegurar el manejo efectivo de incidentes y problemas de vulnerabilidad.

  - Distribuidor relaciones-El papel y las responsabilidades de los proveedores en la prevención de incidentes y seguimiento, corrección de fallas de software, y otras áreas.

- Comunicaciones-Requisitos, implantación y operación de emergencia y canales de comunicación de rutina entre los miembros clave de la gestión.

- Legal y temas de investigación penal Cuestiones impulsado por las consideraciones jurídicas y los requisitos o limitaciones resultantes de la participación de los penales organizaciones de investigación durante un incidente.

- Relaciones con el electorado-Respuesta centro de servicios de apoyo y métodos de interacción con los mandantes, incluida la formación y la sensibilización, gestión de configuración, y la autenticación.

- Programa de investigación e interacción-Identificación de las actividades de investigación existentes y las necesidades y la justificación de la investigación necesaria en relación con las actividades del centro de respuesta.

- Modelo de la amenaza-Desarrollo de un modelo básico que caracteriza a las amenazas y los riesgos potenciales para ayudar a centrar las actividades de reducción de riesgos y el progreso en las actividades.

- Cuestiones externas-Los factores que están fuera del control directo de la empresa (por ejemplo, la legislación, la política, los requisitos de procedimiento), pero que podrían afectar al funcionamiento y eficacia de las actividades de la empresa.

- Determine si el incidente de seguridad en el proceso de gestión de forma adecuada las interfaces con las funciones de organización clave, incluyendo la mesa de ayuda, los proveedores de servicios externos y de gestión de red.

- Evaluar si el proceso de gestión de incidentes de seguridad incluye los siguientes elementos clave:

  - Detección de eventos.

- Correlación de eventos y la evaluación de la amenaza o incidente.
- Resolución de la amenaza, o creación de órdenes de trabajo y la progresividad.
- Criterios para iniciar el proceso de la organización CERT.
- Verificación y niveles necesarios de la documentación de la resolución.
- Posterior a la remediación de análisis.
- Para el trabajo y la incidencia de cierre

DS5.7 Protección de la Tecnología de Seguridad

Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridadinnecesaria.

6.1.4 Proceso de autorización para los servicios de procesamiento de información

Control

Se debería definir e implementar un proceso de automatización de la dirección para nuevos servicios de procesamiento de la información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.

b) Cuando es necesario, el hardware y el software se debería verificar para asegurar que son compatible con otros componentes del sistema.

c) La utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles, computadoras domesticas o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y deberían identificar e implementar los controles necesarios.

9.1.6 Áreas de carga, despacho y acceso público

Control

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por dondepueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible,aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

Guía de implementación

Se recomienda considerar las siguientes directrices

a) Se debería restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado.

b) El área de despacho y carga se debería designar de forma tal que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

c) Las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas.

d) El material que llega se debería inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.

e) El material que llega se debería registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.

f) Los envíos entrantes y salientes se deberían separar físicamente, cuando sea posible.

9.2.1 Ubicación y protección de los equipos

Control

Los equipos deberían estar ubicados o protegidos para reducir el riesgo debido a amenazas opeligros del entorno, y las oportunidades de acceso no autorizado.

Guía de implementación

Se recomienda considerar las siguientes directrices para la protección de los equipos:

a) Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo.

b) Los servicios de procesamiento de información que manejan datos sensibles, deberíanestar ubicados de forma tal que se reduzca el riesgo de visualización de la información-por personas no autorizadas durante su uso, y los sitios de almacenamiento sedeberían asegurar para evitar el acceso no autorizado.

c) Los elementos que requieran protección especial deberían estar aislados para reducir elnivel general de protección requerida de los demás elementos.

d) Se recomienda adoptar controles para minimizar el riesgo de amenazas físicaspotenciales, por ejemplo robo, incendio, explosión, humo, agua (o falla en el suministrode agua), polvo, vibración, efectos químicos, interferencia con el suministro eléctrico,interferencia en las comunicaciones, radiación electromagnética y vandalismo.

e) Se deberían establecer directrices para comer, beber y fumar en las cercanías de losservicios de procesamiento de información.

f) Es conveniente monitorear las condiciones ambientales, como temperatura y humedad,para determinar las condiciones que podrían afectar adversamente el funcionamiento delos servicios de procesamiento de información.

g) Se debería aplicar protección contra rayos a todas las edificaciones y adaptar filtrosprotectores a las fuentes de energía entrantes y a las líneas de comunicación.

h) Es recomendable considerar la utilización de métodos especiales de protección paraequipos en ambientes industriales, tales como membranas para los teclados.

i) Los equipos de procesamiento de información sensible deberían estar protegidos paraminimizar el riesgo de fuga de información debido a filtración.

9.2.3 Seguridad del cableado

Control

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soportea los servicios de información deberían estar protegidos contra interceptaciones o daños.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para la seguridad del cableado:

a) Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada.

b) El cableado de la red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas.

c) Los cables de energía deberían estar separados de los cables de comunicaciones para evitar interferencia.

d) Se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones accidentales de cables erróneos a la red.

e) Es recomendable emplear un plano del cableado para reducir la posibilidad de errores.

f) Para sistemas críticos o sensibles considerar controles adicionales incluyendo:

1) Instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación.

2) Uso de medios alternos de enrutamiento y / o transmisión que suministren seguridad adecuada.

3) Uso de cableado de fibra óptica.

4) Uso de cubiertas (blindaje) electromagnéticas para proteger los cables.

5) Inicio de reconocimientos técnicos e inspecciones físicas en busca de dispositivos no autorizados conectados al cableado.

6) Acceso controlado a los módulos de cableado (patch panel) y a cuartos de cableado.

10.6.2 Seguridad de los servicios de la red

Control

En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir lascaracterísticas de seguridad, los niveles de servicio y los requisitos de gestión de todos losservicios de la red, sin importar si los servicios se prestan en la organización o se contratanexternamente.

Guía de implementación

La capacidad del proveedor del servicio de red para gestionar los servicios acordados de formasegura se debería determinar y monitorear regularmente, y se debería acordar el derecho aauditoría.

Se deberían identificar las disposiciones de seguridad necesarias para servicios particulares,tales como las características de seguridad, los niveles de servicio y los requisitos de gestión.La organización debería garantizar que los proveedores de servicios de red implementan estasmedidas.

10.7.4 Seguridad de la documentación del sistema

Control

La documentación del sistema debería estar protegida contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) la documentación del sistema se debería almacenar con seguridad.

b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.

c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

10.10.1 Registro de auditorías

Control

Se deberían elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.

Guía de implementación

Los registros para auditoría deberían incluir, cuando corresponda.

a) identificación (ID) de usuario.

b) fecha, hora y detalles de los eventos clave, por ejemplo registro de inicio y registro de cierre.

c) identidad o ubicación de la terminal, si es posible.

d) registros de los intentos aceptados y rechazados de acceso al sistema.

e) registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.

f) cambios en la configuración del sistema.

g) uso de privilegios.

h) uso de las utilidades y aplicaciones del sistema.

i) archivos a los que se ha tenido acceso y tipo de acceso.

j) direcciones y protocolos de red.

k) alarmas originadas por el sistema de control del acceso.

l) activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

10.10.3 Protección de la información del registro

Control

Los servicios y la información de la actividad de registro se deberían proteger contra el accesoo la manipulación no autorizados.

Guía de implementación

Los controles deberían tener como objeto la protección contra cambios no autorizados yproblemas operativos con el servicio de registro incluyendo:

a) Alteraciones en los tipos de mensaje que se registran.

b) Archivos de registro que se editan o eliminan.

c) Capacidad de almacenamiento de los medios de archivo de registro que se exceden, lo que resulta en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

Puede ser necesario archivar algunos registros para auditoría como parte de la política deretención de registros o debido a los requisitos para recolectar y conservar evidencia.

10.10.4 Registros del administrador y del operador

Control

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

Guía de implementación

Los registros deberían incluir:

a) La hora en que ocurrió el evento (exitoso o fallido).

b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).

c) Cuál cuenta y cuál administrador u operador estuvo involucrado.

d) Cuáles procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

10.10.5 Registro de fallas

Control

Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas.

Guía de implementación

Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación. Deberían existir reglas claras para el manejo de las fallas reportadas, incluyendo:

a) revisión de los registros de fallas para garantizar que las éstas se han resuelto satisfactoriamente.

b) revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

Se debería asegurar que el registro de errores está habilitado, si esta función del sistema está disponible.

10.10.6 Sincronización de relojes

Control

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de laorganización o del dominio de seguridad deberían estar sincronizados con una fuente detiempo exacta y acordada.

Guía de implementación

Cuando un computador o un dispositivo de comunicaciones tiene la capacidad para operar unreloj en tiempo real, dicho reloj se debería establecer como el estándar acordado, por ejemploel tiempo coordinado universal (UTC) o el tiempo estándar local. Debido a que se sabe quealgunos relojes varían con el paso del tiempo, debería existir un procedimiento que verifique ycorrija cualquier variación significativa.

La interpretación correcta del formato fecha / hora es importante para garantizar que la marcade tiempo refleja la fecha/hora real. Es conveniente tener en cuenta las especificacioneslocales (por ejemplo el horario de verano).

11.3.2 Equipo de usuario desatendido

Control

Los usuarios deberían asegurarse de que los equipos desatendidos tengan protección apropiada.

Guía de implementación

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña.

b) realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal).

c) cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña.

11.3.3 Política de escritorio despejado y de pantalla despejada

Control

Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

Guía de implementación

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) cuando no se requiere la información sensible o crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave (idealmente una caja fuerte, un gabinete u otro mueble de seguridad), especialmente cuando la oficina está vacía.

b) las sesiones de los computadores y los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un *token* o un mecanismo similar de autenticación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando.

c) se deberían proteger los puntos de entrada y salida de correo y las máquinas de facsímil desatendidas.

d) es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, etc.).

e) los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.

11.4.3 Identificación de los equipos en las redes

Control

La identificación automática de los equipos se debería considerar un medio para autenticarconexiones de equipos y ubicaciones específicas.

Guía de implementación

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente sepueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado aéste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estosidentificadores deberían indicar con claridad a qué red está permitido conectar el equipo, siexiste más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesarioconsiderar la protección física del equipo para mantener la seguridad del identificador de éste.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto

Control

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estarcontrolado.

Guía de implementación

Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyenel uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico alpuerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos dediagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador delservicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o dered, que no se requieren específicamente para la funcionalidad del negocio, se deberíaninhabilitar o retirar.

11.5.1 Procedimientos de registro de inicio seguro

Control

El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.

Guía de implementación

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.

b) Mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados.

c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.

d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta.

e) Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar:

   1) Registrar intentos exitosos y fallidos.

   2) Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica.

   3) Desconectar las conexiones de enlaces de datos.

   4) Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio.

   5) Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege.

f) Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación;

g) Mostrar la siguiente información al terminar un registro de inicio exitoso:

   1) Fecha y hora del registro de inicio exitoso previo.

   2) Detalles de los intentos fallidos de registro de inicio desde el último registro exitoso.

h) No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos.

i) No transmitir contraseñas en texto claro en la red.

11.5.4 Uso de las utilidades del sistema

Control

Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

Guía de aplicación

Se recomienda considerar la siguiente directriz para el uso de las utilidades del sistema:

a) uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.

b) separación de las utilidades del sistema del software de aplicaciones.

c) limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.

d) autorización del uso ad hoc de las utilidades del sistema

e) limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado.

f) registro de todo uso de las utilidades del sistema.

g) definición y documentación de los niveles de autorización para las utilidades del sistema.

h) retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.

i) no poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

11.5.5 Tiempo de inactividad de la sesión

Control

Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad.

Guía de implementación

Una utilidad de tiempo de inactividad debería despejar la pantalla de sesión y también, tal vezmás tarde, cerrar tanto la sesión de la aplicación como la de red después de un periododefinido de inactividad. La dilación del tiempo de inactividad debería reflejar los riesgos deseguridad del área, la clasificación de la información que se maneja y las aplicaciones que seutilizan, así como los riesgos relacionados con los usuarios del equipo.

Algunos sistemas pueden suministrar una forma limitada de utilidad de tiempo de inactividad lacual despeja la pantalla y evita el acceso no autorizado, pero no cierra las sesiones deaplicación ni de red.

11.5.6 Limitación del tiempo de conexión

Control

Se deberían utilizar restricciones en los tiempos de conexión para brindar seguridad adicionalpara las aplicaciones de alto riesgo.

Guía de implementación

Se deberían tener en cuenta los controles de tiempo para las aplicaciones sensibles decomputador, especialmente las de lugares de alto riesgo, por ejemplo áreas públicas o externasque están fuera de la gestión de seguridad de la organización. Los siguientes son algunosejemplos de estas restricciones:

a) Uso de espacios de tiempo predeterminados, por ejemplo, para transmisiones de lotes de archivos, o uso de sesiones interactivas de corta duración.

b) Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.

c) Considerar la repetición de la autenticación a intervalos determinados.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación.

b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible.

11.7.1 Computación y comunicaciones móviles

Control

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Guía de implementación

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (*notebooks*), microcomputadores de bolsillo (*palmtops*), y computadores portátiles pesados (*laptops*), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos sin protección.

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio. Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información. Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes debería tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y / o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

11.7.2 Trabajo remoto

Control

Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guía de implementación

Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo, robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) la seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local.

b) el entorno físico de trabajo remoto propuesto.

c) los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno.

d) la amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos.

e) el uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.

f) las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.

g) el acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley.

h) los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.

i) protección antivirus y requisitos de barreras contra fuego (firewall).

Las directrices y disposiciones a considerar deberían incluir las siguientes:

a) disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización.

b) definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.

c) disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto.

d) seguridad física.

e) reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

f) disposición de soporte y mantenimiento de hardware y software.

g) disposición de pólizas de seguros.

h) procedimientos para el respaldo y la continuidad del negocio.

12.4.1 Control del software operativo

Control

Se deberían establecer procedimientos para controlar la instalación de software en los sistemasoperativos.

Guía de implementación

Para minimizar los riesgos de corrupción de los sistemas operativos, se deberían teneren cuenta las siguientes directrices para controlar los cambios:

a) La actualización del software operativo, las aplicaciones y las librerías de los programas sólo deberían ser realizadas por administradores capacitados y con la debida autorización de la dirección.

b) Los sistemas operativos únicamente deberían contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores.

c) El software de las aplicaciones y del sistema operativo sólo se deberían implementar después del ensayo exhaustivo y exitoso; los ensayos deberían incluir pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, igualmente se deberían efectuar en sistemas separados; se debería garantizar que todas las librerías fuente del programa correspondiente estén actualizadas.

d) Se debería usar un sistema de control de configuración para mantener el control el software implementado, así como de la documentación del sistema.

e) Es conveniente instaurar una política de estrategia de restauración al estado anterior antes de implementar los cambios.

f) Se debería conservar un registro para auditoría de todas las actualizaciones de las librerías de los programas operativos.

g) Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.

h) Las versiones antiguas del software se deberían archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

El software suministrado por el vendedor utilizado en los sistemas operativos se deberíamantener en el nivel con soporte del proveedor. Con el tiempo, los vendedores de softwaredejarán de dar soporte a las versiones antiguas del software. La organización deberíaconsiderar los riesgos de depender de software sin soporte.

En toda decisión para mejorar a una nueva versión se debería contar con los requisitos delnegocio para el cambio, y la seguridad de la nueva versión, es decir, la introducción de nuevafuncionalidad en el sistema o la cantidad y gravedad de los problemas de seguridad queafectan a esta versión. Los parches de software se deberían aplicar cuando pueden ayudar aeliminar o reducir las debilidades de la seguridad.

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos desoporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedorse deberían monitorear.

El software de computador puede depender de software y módulos suministradosexternamente, lo cual se debería monitorear y controlar para evitar cambios no autorizados quepuedan introducir debilidades de seguridad.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

   1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

   2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red.

   3) aumentar el monitoreo para detectar o prevenir los ataques reales.

   4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.

j) se deberían tratar primero los sistemas con alto riesgo.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

15.2.2 Verificación del cumplimiento técnico

Control

Los sistemas de información se deberían verificar periódicamente para determinar elcumplimiento con las normas de implementación de la seguridad.

Guía de implementación

La verificación del cumplimiento técnico se debería realizar bien sea manualmente (con soportede las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas conexperiencia y / o con la ayuda de herramientas automáticas que generan un informe técnicopara la interpretación posterior por parte del especialista técnico.

Si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tenercuidado puesto que dichas actividades pueden poner en peligro la seguridad del sistema. Talespruebas se deberían planificar, documentar y ser repetibles.

La verificación del cumplimiento técnico únicamente la deberían realizar personas autorizadas ycompetentes o bajo supervisión de dichas personas.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

Guía de implementación

Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativos y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

Guías de Aseguramiento

- Averiguar y confirmar si las políticas y procedimientos se han establecido para eliminar las consecuencias de violaciones de seguridad (en concreto para hacer frente a los controlesgestión de configuración, acceso a las aplicaciones, seguridad de los datos y requisitos de seguridad física).

- Inspeccione los registros de control de la concesión y la aprobación de acceso y registro de intentos fallidos, cierres patronales, el acceso autorizado a archivos confidenciales y / o datos, y física acceso a las instalaciones.

- Averiguar y confirmar si las características de diseño de seguridad de facilitar reglas de contraseña (por ejemplo, la longitud máxima, los personajes, la caducidad, la reutilización).
- Averiguar y confirmar si el control requiere revisiones anuales de gestión de elementos de seguridad para el acceso físico y lógico a los archivos y datos.
- Verifique que el acceso es autorizado y aprobado debidamente.
- Revise los informes de seguridad generados por las herramientas de sistema de prevención de ataques de red vulnerabilidad penetración.

DS5.8 Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución,certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de lasllaves contra modificaciones y divulgación no autorizadas.

10.8.4 Mensajería electrónica

Control

La información contenida en la mensajería electrónica debería tener la protección adecuada.

Guía de implementación

Las consideraciones de seguridad para la mensajería electrónica deberían incluir lassiguientes:

a) Proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios.

b) Garantizar que la dirección y el transporte del mensaje son correctos.

c) Confiabilidad general y disponibilidad del servicio.

d) Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas.

e) Obtención de aprobación antes de utilizar servicios públicos externos como lamensajería instantánea o el compartir archivos.

f) Niveles más sólidos de autenticación que controlen el acceso desde redes accesibles alpúblico.

12.2.3 Integridad del mensaje

Control

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

Guía de implementación

Se debería realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

12.3.1 Política sobre el uso de controles criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Guía de implementación

Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

a) el enfoque de la dirección hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.

b) con base en la evaluación de riesgos, se debería identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.

c) uso de encriptación para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos o a través de las líneas de comunicación.

d) enfoque para la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.

e) funciones y responsabilidades, por ejemplo, quién es responsable de:

   1) la implementación de la política.

   2) la gestión de claves, incluyendo su generación.

f) normas que se han de adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio).

g) impacto de la utilización de información encriptada sobre los controles que depende de la inspección del contenido (por ejemplo, detección de virus).

Cuando se implementa la política de encriptación de la organización, es conveniente tener en mente los reglamentos y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los aspectos del flujo trans-fronterizo de información encriptada.

Los controles criptográficos se pueden utilizar para lograr diferentes objetivos de seguridad, por

ejemplo:

a) confidencialidad: uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.

b) integridad / autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.

c) no-repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

12.3.2 Gestión de claves

Control

Se debería establecer la gestión de claves para apoyar el uso de técnicas criptográficas en laorganización.

Guía de implementación

Todas las claves criptográficas deberían tener protección contra modificación, pérdida ydestrucción. Además, las claves privadas y secretas necesitan protección contra divulgación noautorizada. El equipo usado para generar, almacenar y archivar las claves debería estarprotegido por medios físicos.

Un sistema de gestión de claves se debería basar en un conjunto acordado de normas,procedimientos y método seguros para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b) Generar y obtener certificados de claves públicas.

c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.

d) Almacenar las claves, incluyendo la forma en que los usuarios autorizados tendrán acceso a ellas.

e) Cambiar o actualizar las claves incluyendo reglas sobre cuándo cambiarlas y cómo hacerlo.

f) Tratar las claves perdidas.

g) Revocar las claves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización (en cuyo caso las claves también se deberían archivar).

h) Recuperar claves pérdidas o corruptas como parte de la gestión de continuidad del negocio; por ejemplo, para la recuperación de información encriptada.

i) Archivar claves, por ejemplo para la información archivada o con copia de respaldo.

j) Destrucción de claves.

k) Registro y auditoría de las actividades relacionadas con la gestión de claves.

Para reducir la probabilidad de poner en peligro, activar o desactivar se deberían definir fechaspara las claves de modo que sólo se puedan utilizar durante un periodo de tiempo limitado.

Este período dependería de las circunstancias en las cuales se usa el control criptográfico y delriesgo percibido.

Además de las claves privadas y secretas con gestión segura, también se debería pensar en laautenticidad de las claves públicas. Este proceso de autenticación se puede hacer concertificados de claves públicas que normalmente son emitidos por una autoridad decertificación, la cual debe ser una organización reconocida con controles y procedimientosidóneos establecidos para proporcionar el grado requerido de confianza.

El contenido de los acuerdos o contratos de servicios con proveedores externos de servicioscriptográficos, por ejemplo con una autoridad de certificación, deberían comprender aspectosde responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la prestación delos servicios.

15.1.6 Reglamento de los controles criptográficos

Control

Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

Guía de implementación

Se recomienda tener presentes los siguientes elementos para el cumplimiento con acuerdos, leyes y reglamentos pertinentes:

a) Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de las funciones criptográficas.

b) Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.

c) Restricciones al uso de encriptación.

d) Métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

Se debería buscar asesoría legal para garantizar el cumplimiento con las leyes y los reglamentos nacionales. Antes de desplazar la información encriptada o los controles criptográficos a otros países, se debería tener asesoría legal.

Guías de Aseguramiento

- Determinar si un ciclo definido de gestión de procesos clave de la vida existe. El proceso debe incluir:
  - Tamaño mínimo de la clave necesaria para la generación de claves seguras.
  - El uso de algoritmos de generación de claves necesarias.

- Identificación de las normas necesarias para la generación de claves.
- Fines para los que las claves deben ser utilizadas y restringido.
- Los períodos permitidos de uso o cursos de la vida activa para las llaves.
- Los métodos aceptables de distribución de claves.
- Copia de seguridad de clave de archivo, y la destrucción.

- Evaluar si los controles sobre las claves privadas existen para hacer cumplir su confidencialidad e integridad. Se debe considerar lo siguiente:
  - Almacenamiento de claves de firma privada dentro de fronteras seguras dispositivos criptográficos (por ejemplo, FIPS 140-1, ISO 15782-1, ANSI X9.66).
  - Las claves privadas no se exporta desde un módulo criptográfico seguro.
  - Las claves privadas copia de seguridad, almacenados y recuperados por personal autorizado, haciendo uso de control dual en un entorno físicamente seguro.
- Averiguar y confirmarsi la organización ha puesto en marcha la clasificación de la información y los controles de protección asociados a la información que dan cuenta de la necesidades de la organización para compartir o restringir la información y los impactos organizacionales asociados con tales necesidades.
- Determinar si los procedimientos están definidos para asegurar que el etiquetado de la información y el manejo se realiza de acuerdo con la información de la organización esquema de clasificación.

DS5.9 Prevención, Detección y Corrección de Software Malicioso

Poner medidas preventivas, detectives y correctivas (en especial contar con parches de seguridad y control de virus actualizados) entoda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correobasura).

10.4.1 Controles contra códigos maliciosos

Control

Se deberían implementar controles de detección, prevención y recuperación para protegercontra códigos maliciosos, así como procedimientos apropiados de concientización de losusuarios.

Guía de implementación

La protección contra códigos maliciosos se debería basar en software de detección yreparación de códigos maliciosos, conciencia sobre seguridad, acceso apropiado al sistema ycontroles en la gestión de cambios. Se recomienda considerar las siguientes directrices:

a) Establecer una política formal que prohíba el uso de software no autorizado.

b) Establecer una política formal para la protección contra los riesgos asociados con la obtención de archivos y software, bien sea desde o a través de redes externas o cualquier otro medio, indicando las medidas de protección que se deberían tomar.

c) Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

d) Instalación y actualización regular del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios, como control preventivo o de forma rutinaria; las verificaciones realizadas deberían incluir:

1) Verificación de la presencia de códigos maliciosos en todos los archivos en medios ópticos o electrónicos y archivos recibidos en las redes antes de su uso.

2) Verificación de la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso; esta verificación se debería efectuar en diferentes lugares, por ejemplo en los servidores de correo electrónico, los computadores de escritorio y cuando ingresan a la red de la organización.

3) Verificación de las páginas web para comprobar la presencia de códigos maliciosos.

e) Definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas, la formación sobre su uso, el reporte y la recuperación debido a ataques de códigos maliciosos.

f) Preparación de planes adecuados para la continuidad del negocio con el fin de recuperarse de los ataques de códigos maliciosos, incluyendo todos los datos y el soporte de softwarenecesario y las disposiciones para la recuperación.

g) Implementación de procedimientos para recolectar información con regularidad, como la suscripción a sitios web de verificación y / o listados de correo que suministren información sobre los códigos maliciosos nuevo.

h) Implementación de procedimientos para verificar la información relacionada con códigos maliciosos y garantizar que los boletines de advertencia sean exactos e informativos; los directores deberían garantizar que se utilizan fuentes calificadas, por ejemplo diarios reconocidos, sitios confiables de Internet o proveedores de software de protección contra códigos maliciosos para diferenciar entre falsas alarmas y códigos maliciosos reales; todos los usuarios deberían conocer el problema de los falsas alarmas y quéhacer al recibirlas.

10.4.2 Controles contra códigos móviles

Control

Cuando se autoriza la utilización de códigos móviles, la configuración debería asegurar quedichos códigos operan de acuerdo con la política de seguridad claramente definida, y sedebería evitar la ejecución de los códigos móviles no autorizados.

Guía de implementación

Se recomienda tener en cuenta las siguientes consideraciones para la protección contracódigos móviles que ejecutan acciones no autorizadas:

a) Ejecución de los códigos móviles en un entorno con aislamiento lógico.

b) Bloqueo de cualquier uso de códigos móviles.

c) Bloqueo de la recepción de códigos móviles.

d) Activación de medidas técnicas, según estén disponibles, en un sistema específico para garantizar la gestión del código móvil.

e) Control de recursos disponibles para el acceso a códigos móviles.

f) Controles criptográficos para autenticar de forma única el código móvil.

Guías de Aseguramiento

- Averiguar y confirmar si, una política de prevención de software malicioso está establecida y documentada, y en toda la organización.

- Asegúrese de que los controles automatizados se han implementado para proporcionar protección contra virus y que violaciones se comunican adecuadamente.
- Infórmese de los miembros clave de si son conscientes de la política de prevención de software malintencionado y su responsabilidad de garantizar el cumplimiento.
- De una muestra de estaciones de trabajo de usuario, observar si una herramienta de protección contra virus se ha instalado e incluye los archivos de definición de virus y la última vez que las definiciones se han actualizado.
- Averiguar y confirmar si el software de protección es de distribución central (la versión y el nivel de parche), utilizando una configuración centralizada y el cambiogestión de procesos.
- Revisar el proceso de distribución para determinar la efectividad operativa.
- Averiguar y confirmar si la información sobre nuevas amenazas potenciales se revisa periódicamente y evaluados y, en caso necesario, actualizados a mano a los archivos de definición de virus.
- Revisar el proceso de revisión y evaluación para determinar la efectividad operativa.
- Averiguar y confirmar si el correo electrónico entrante se filtra adecuadamente contra la información no solicitada.
- Revisar el proceso de filtración para determinar la efectividad operativa, o revisar el proceso automatizado establecido para filtrar los propósitos.Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS5.10 Seguridad de la Red

Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad,segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

   1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

   2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

   3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

   4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

10.6.1 Controles de las redes

Control

Las redes de deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

Guías de implementación

Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa por las redes debería estar separada de la operaciones de computador, según sea apropiado (**10.1.3 Distribución (Segregación) de funciones** de la cual se hace referencia en el primer ítem de la guía).

b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remostos, incluyendo los equipos en áreas de usuario.

c) Es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas; también se puede requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.

d) Se debería aplicar el registro y el monitoreo adecuado para permitir el registro de acciones de seguridad pertinente.

e) Se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

10.6.2 Seguridad de los servicios de la red

Control

En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir lascaracterísticas de seguridad, los niveles de servicio y los requisitos de gestión de todos losservicios de la red, sin importar si los servicios se prestan en la organización o se contratanexternamente.

Guía de implementación

La capacidad del proveedor del servicio de red para gestionar los servicios acordados de formasegura se debería determinar y monitorear regularmente, y se debería acordar el derecho aauditoría.

Se deberían identificar las disposiciones de seguridad necesarias para servicios particulares,tales como las características de seguridad, los niveles de servicio y los requisitos de gestión.La organización debería garantizar que los proveedores de servicios de red implementan estasmedidas.

11.4.1 Política de uso de los servicios en red

Control

Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamenteautorizados.

Guía de implementación

Se debería formular una política con respecto al uso de las redes y los servicios de red. Estapolítica debería abarcar:

a) Las redes y los servicios de red a los cuales se permite el acceso.

b) Los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red.

c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red.

d) Los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de Internet o a un sistema remoto).

La política sobre el uso de los servicios de red debería ser consistente con la política de controlde acceso de la organización.

11.4.2 Autenticación de usuarios para conexiones externas

Control

Se deberían emplear métodos apropiados de autenticación para controlar el acceso deusuarios remotos.

Guía de implementación

La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica conbase criptográfica, *token* de hardware o protocolos de desafío / respuesta. Las posiblesimplementaciones de dichas técnicas se pueden encontrar en diversas soluciones de redprivada virtual (VPN). Las líneas privadas dedicadas también se pueden emplear para brindaraseguramiento de la fuente de las conexiones.

Los procedimientos y controles de devolución de marcación, por ejemplo empleando módemsde retorno de marcación, pueden suministrar protección contra conexiones no deseadas o noautorizadas a los servicios de procesamiento de información de la organización. Este tipo decontrol autentica a los usuarios tratando de establecer una conexión con una red de laorganización desde sitios remotos. Cuando se usa este control, la organización no deberíautilizar servicios de red que incluyen envío de llamada o, si lo hacen, deberían desactivar el usode dichas características para evitar las debilidades asociadas con el envío de llamada.

Elproceso de devolución de llamada debería garantizar que realmente se produce unadesconexión en el lado de la organización. De otro modo, el usuario remoto debería mantenerla línea abierta pretendiendo que ha ocurrido la verificación de la devolución de la llamada. Losprocedimientos y controles de devolución de la llamada se deberían probar en su totalidad paradeterminar esta posibilidad.

La autenticación del nodo puede servir como un medio alterno para la autenticación de gruposde usuarios remotos cuando están conectados a un servicio seguro de computador compartido. Para la autenticación del nodo se pueden emplear las técnicas criptográficas, por ejemplo lasbasadas en certificados de máquina. Esto forma parte de varias soluciones basadas en la redprivada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso aredes inalámbricas. En particular, es necesario tener cuidado especial en la selección de loscontroles para redes inalámbricas debido a las grandes oportunidades para la interceptación einserción no detectadas en el tráfico de la red.

11.4.3 Identificación de los equipos en las redes

Control

La identificación automática de los equipos se debería considerar un medio para autenticarconexiones de equipos y ubicaciones específicas.

Guía de implementación

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente sepueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado aéste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estosidentificadores deberían indicar con claridad a qué red está permitido conectar el equipo, siexiste más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesarioconsiderar la protección física del equipo para mantener la seguridad del identificador de éste.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto

Control

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estarcontrolado.

Guía de implementación

Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyenel uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico alpuerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos dediagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador delservicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o dered, que no se requieren específicamente para la funcionalidad del negocio, se deberíaninhabilitar o retirar.

11.4.5 Separación en las redes

Control

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemasde información.

Guía de implementación

Un método para el control en las redes grandes es dividirlas en dominios lógicos de redseparados, por ejemplo, dominios de red internos de la organización y dominios de redexternos, cada uno protegido por un perímetro de seguridad definido. Se puede aplicar unconjunto graduado de controles en diferentes dominios lógicos de red para separar aún más losentornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internasy los activos críticos. Los dominios se deberían definir con base en una evaluación de riesgos yen los diferentes requisitos de seguridad en cada uno de los dominios.

Se puede implementar un perímetro de red instalando una puerta de enlace (*gateway*) seguroentre las dos redes que se van a interconectar para controlar el acceso y el flujo de informaciónentre los dos dominios. Esta puerta de enlace (*gateway*) se debería configurar para filtrar eltráfico entre estos dominios y para bloquear el acceso noautorizado, según la política de control de acceso de la organización. Unejemplo de este tipo de puerta de enlace (*gateway*) es lo que se conoce comúnmente comobarrera de fuego (*firewall*). Otro método para apartar los dominios lógicos separados esrestringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro dela organización.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, porejemplo la conmutación IP. Los dominios separados se pueden implementar entoncescontrolando los flujos de datos de la red usando las capacidades de enrutamiento /conmutación, como por ejemplo las listas de control de acceso.

Los criterios para separar las redes en dominios se deberían basar en la política de control deacceso y en los requisitos de accesoy deberían tener en cuenta loscostos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente depuerta de enlace (*gateway*) o de enrutamiento de red.

Además, la separación de las redes se debería basar en el valor y la clasificación de lainformación almacenada o procesada en la red, los niveles de confianza o los lineamientos delnegocio con el fin de reducir el impacto total de una interrupción del servicio.

También se debería pensar en la separación de las redes inalámbricas procedentes de redesinternas y privadas. Puesto que los perímetros de las redes inalámbricas no están biendefinidos, es recomendable llevar a cabo una evaluación de riesgos en tales casos paraidentificar los controles (por ejemplo, autenticación sólida, métodos criptográficos y selecciónde frecuencia) para mantener la separación de la red.

11.4.6 Control de conexión a las redes

Control

Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras dela organización, se debería restringir la capacidad de los usuarios para conectarse a la red, deacuerdo con la política de control de acceso y los requisitos de aplicación del negocio.

Guía de implementación

Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según serequiera a través de la política de control de acceso.

La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace(*gateway*) de red que filtren el tráfico por medio de tablas o reglas predefinidas. Los siguientesson algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

a) Mensajería, por ejemplo, el correo electrónico.

b) Transferencia de archivos.

c) Acceso interactivo.

d) Acceso a las aplicaciones.

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red conalgunas horas del día o fechas.

11.4.7 Control del enrutamiento en la red

Control

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que lasconexiones entre computadores y los flujos de información no incumplan la política de controlde acceso de las aplicaciones del negocio.

Guía de implementación

Los controles de enrutamiento se deberían basar en mecanismos de verificación para lasdirecciones fuente / destino válidos.

Las puertas de enlace (*gateway*) de seguridad se pueden usar para validar la direcciónfuente/destino en los puntos de control de las redes interna y externa, si se empleantecnologías *proxy* y / o de traducción de dirección de red. Quienes desarrollan laimplementación deberían ser conscientes de las fortalezas y deficiencias de los mecanismosdesplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en lapolítica de control de acceso.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación.

b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible.

Guías de Aseguramiento

- Averiguar y confirmar si, una política de seguridad de red (por ejemplo, siempre y servicios, permite el tráfico, los tipos de conexiones permitidas) se ha establecido y se mantiene.
- Averiguar y confirmar si los procedimientos y directrices para la administración de todos los componentes de redes críticas (por ejemplo, routers de núcleo, zona de distensión, interruptores VPN) establecida y actualizada periódicamente por el personal clave de la administración, y los cambios en la documentación se realiza un seguimiento en la historia del documento.

DS5.11 Intercambio de Datos Sensitivos

Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad decontenido, prueba de envío, prueba de recepción y no repudio del origen

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

   1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

   2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

   3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

   4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

10.6.1 Controles de las redes

Control

Las redes de deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

Guías de implementación

Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa por las redes debería estar separada de la operaciones de computador, según sea apropiado (**10.1.3 Distribución (Segregación) de funciones** de la cual se hace referencia en el primer ítem de la guía).

b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remostos, incluyendo los equipos en áreas de usuario.

c) Es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas; también se puede requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.

d) Se debería aplicar el registro y el monitoreo adecuado para permitir el registro de acciones de seguridad pertinente.

e) Se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

10.6.2 Seguridad de los servicios de la red

Control

En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir lascaracterísticas de seguridad, los niveles de servicio y los requisitos de gestión de todos losservicios de la red, sin importar si los servicios se prestan en la organización o se contratanexternamente.

Guía de implementación

La capacidad del proveedor del servicio de red para gestionar los servicios acordados de formasegura se debería determinar y monitorear regularmente, y se debería acordar el derecho aauditoría.

Se deberían identificar las disposiciones de seguridad necesarias para servicios particulares,tales como las características de seguridad, los niveles de servicio y los requisitos de gestión.La organización debería garantizar que los proveedores de servicios de red implementan estasmedidas.

11.4.1 Política de uso de los servicios en red

Control

Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamenteautorizados.

Guía de implementación

Se debería formular una política con respecto al uso de las redes y los servicios de red. Estapolítica debería abarcar:

a) Las redes y los servicios de red a los cuales se permite el acceso.

b) Los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red.

c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red.

d) Los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de Internet o a un sistema remoto).

La política sobre el uso de los servicios de red debería ser consistente con la política de controlde acceso de la organización.

11.4.2 Autenticación de usuarios para conexiones externas

Control

Se deberían emplear métodos apropiados de autenticación para controlar el acceso deusuarios remotos.

Guía de implementación

La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica conbase criptográfica, *token* de hardware o protocolos de desafío / respuesta. Las posiblesimplementaciones de dichas técnicas se pueden encontrar en diversas soluciones de redprivada virtual (VPN). Las líneas privadas dedicadas también se pueden emplear para brindaraseguramiento de la fuente de las conexiones.

Los procedimientos y controles de devolución de marcación, por ejemplo empleando módemsde retorno de marcación, pueden suministrar protección contra conexiones no deseadas o noautorizadas a los servicios de procesamiento de información de la organización. Este tipo decontrol autentica a los usuarios tratando de establecer una conexión con una red de laorganización desde sitios remotos. Cuando se usa este control, la organización no deberíautilizar servicios de red que incluyen envío de llamada o, si lo hacen, deberían desactivar el usode dichas características para evitar las debilidades asociadas con el envío de llamada. Elproceso de devolución de llamada debería garantizar que realmente se produce unadesconexión en el lado de la organización. De otro modo, el usuario remoto debería mantenerla línea abierta pretendiendo que ha ocurrido la verificación de la devolución de la llamada. Losprocedimientos y controles de devolución de la llamada se deberían probar en su totalidad paradeterminar esta posibilidad.

La autenticación del nodo puede servir como un medio alterno para la autenticación de gruposde usuarios remotos cuando están conectados a un servicio seguro de computador compartido. Para la autenticación del nodo se pueden emplear las técnicas criptográficas, por ejemplo lasbasadas en certificados de máquina. Esto forma parte de varias soluciones basadas en la redprivada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso aredes inalámbricas. En particular, es necesario tener cuidado especial en la selección de loscontroles para redes inalámbricas debido a las grandes oportunidades para la interceptación einserción no detectadas en el tráfico de la red.

11.4.3 Identificación de los equipos en las redes

Control

La identificación automática de los equipos se debería considerar un medio para autenticarconexiones de equipos y ubicaciones específicas.

Guía de implementación

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente sepueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado aéste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estosidentificadores deberían indicar con claridad a qué red está permitido conectar el equipo, siexiste más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesarioconsiderar la protección física del equipo para mantener la seguridad del identificador de éste.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto

Control

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estarcontrolado.

Guía de implementación

Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyenel uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico alpuerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos dediagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador delservicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o dered, que no se requieren específicamente para la funcionalidad del negocio, se deberíaninhabilitar o retirar.

11.4.5 Separación en las redes

Control

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemasde información.

Guía de implementación

Un método para el control en las redes grandes es dividirlas en dominios lógicos de redseparados, por ejemplo, dominios de red internos de la organización y dominios de redexternos, cada uno protegido por un perímetro de seguridad definido. Se puede aplicar unconjunto graduado de controles en diferentes dominios lógicos de red para separar aún más losentornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internasy los activos críticos. Los dominios se deberían definir con base en una evaluación de riesgos yen los diferentes requisitos de seguridad en cada uno de los dominios.

Se puede implementar un perímetro de red instalando una puerta de enlace (*gateway*) seguroentre las dos redes que se van a interconectar para controlar el acceso y el flujo de informaciónentre los dos dominios. Esta puerta de enlace (*gateway*) se debería configurar para filtrar eltráfico entre estos dominios y para bloquear el acceso noautorizado, según la política de control de acceso de la organización. Unejemplo de este tipo de puerta de enlace (*gateway*) es lo que se conoce comúnmente comobarrera de fuego (*firewall*). Otro método para apartar los dominios lógicos separados esrestringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro dela organización.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, porejemplo la conmutación IP. Los dominios separados se pueden implementar entoncescontrolando los flujos de datos de la red usando las capacidades de enrutamiento / conmutación, como por ejemplo las listas de control de acceso.

Los criterios para separar las redes en dominios se deberían basar en la política de control deacceso y en los requisitos de accesoy deberían tener en cuenta loscostos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente depuerta de enlace (*gateway*) o de enrutamiento de red.

Además, la separación de las redes se debería basar en el valor y la clasificación de lainformación almacenada o procesada en la red, los niveles de confianza o los lineamientos delnegocio con el fin de reducir el impacto total de una interrupción del servicio.

También se debería pensar en la separación de las redes inalámbricas procedentes de redesinternas y privadas. Puesto que los perímetros de las redes inalámbricas no están biendefinidos, es recomendable llevar a cabo una evaluación de riesgos en tales casos paraidentificar los controles (por ejemplo, autenticación sólida, métodos criptográficos y selecciónde frecuencia) para mantener la separación de la red.

11.4.6 Control de conexión a las redes

Control

Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras dela organización, se debería restringir la capacidad de los usuarios para conectarse a la red, deacuerdo con la política de control de acceso y los requisitos de aplicación del negocio.

Guía de implementación

Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según serequiera a través de la política de control de acceso.

La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace(*gateway*) de red que filtren el tráfico por medio de tablas o reglas predefinidas. Los siguientesson algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

a) Mensajería, por ejemplo, el correo electrónico.

b) Transferencia de archivos.

c) Acceso interactivo.

d) Acceso a las aplicaciones.

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red conalgunas horas del día o fechas.

11.4.7 Control del enrutamiento en la red

Control

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que lasconexiones entre computadores y los flujos de información no incumplan la política de controlde acceso de las aplicaciones del negocio.

Guía de implementación

Los controles de enrutamiento se deberían basar en mecanismos de verificación para lasdirecciones fuente /destino válidos.

Las puertas de enlace (*gateway*) de seguridad se pueden usar para validar la direcciónfuente/destino en los puntos de control de las redes interna y externa, si se empleantecnologías *proxy* y / o de traducción de dirección de red. Quienes desarrollan laimplementación deberían ser conscientes de las fortalezas y deficiencias de los mecanismosdesplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en lapolítica de control de acceso.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación.

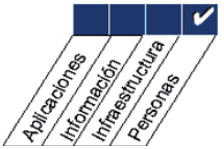
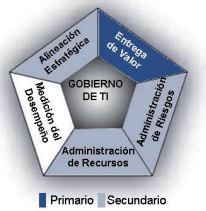
b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible.

Guías de Aseguramiento

- Averiguar y confirmar si la transmisión de datos fuera de la organización requieren formato encriptado antes de la transmisión.
- Averiguar y confirmar si los datos corporativos se clasifican según el nivel de exposición y el esquema de clasificación (por ejemplo, sensible confidencial).
- Averiguar y confirmar si el tratamiento de datos sensibles es controlado a través de controles de aplicación que validar la transacción antes de la transmisión.
- Revisar que los registros de aplicación o procesamiento se detiene para las transacciones no válida o incompleta.

DS7 Educar y Entrenar a los Usuarios

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar lasnecesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición yejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo deentrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimientode los controles clave tales como las medidas de seguridad de los usuarios.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS7.1 Identificación de Necesidades de Entrenamiento y Educación

Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Averiguar y confirmar si un plan de formación y desarrollo profesional de los miembros del personal de TI existente.
- Obtener y revisar el plan de estudios para la integridad (por ejemplo, la profundidad y amplitud de la cobertura, la frecuencia de las clases, horario de clases, la complejidad de la clase, el origen de la formación-proveedor local de la escuela o instituto de comercio).
- Obtener y revisar el calendario de formación.
- Obtener y revisar el presupuesto de formación.
- Obtenga una copia de la terminación de la prueba, puntuación y confirmación de asistencia (porejemplo, pruebas en línea curso de formación de los exámenes y la asistencia).
- Determinar el proceso de gestión para desarrollar y mantener un inventario de habilidades.
- Obtener y revisar el catálogo de inventario de habilidades para determinar si las habilidadescatalogado mapa para los sistemas implementados.

- Determinar que la base de datos de conocimientos es el conocimiento actual y disponible se mantiene como corriente.
- Inspeccione la estrategia de capacitación para asegurar que las necesidades de formación seincorporarán en los planes de los usuarios en el desempeño individual.
- Inspeccione la documentación que detalla la obligación de analizar las causas fundamentales, incluidos los de formación, de las salidas de servicio de mesa.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS7.2 Impartición de Entrenamiento y Educación

Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismosde impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratista y los usuarios de terceras partes deberían recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinente para sus funciones laborales.

Guías de implementación

La formación en concientización debería empezar por un proceso formal de introducción diseñado para presentar las políticas de seguridad de la organización y las expectativas antes de otorgar el acceso a la información o a los servicios.

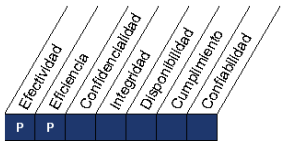
Es recomendable que la formación continua incluya los requisitos de seguridad, las responsabilidades las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario.

Guías de Aseguramiento

- Revisar el programa de entrenamiento, y confirme que cumple con las necesidades de formación.
- Asegúrese de que los recursos adecuados estén disponibles para impartir formación.
- Analizar una muestra de los programas de capacitación y verificar:
  - Contenido vs objetivos.
  - La asistencia real vs planeado.
  - Satisfacción de asistentes.
  - Aplicación de los comentarios recibidos.

DS8 Administrar la Mesa de Servicio y los Incidentes.

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio biendiseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesade servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raiz y resolución. Los beneficios del negocioincluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causaraíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS8.1 Mesa de Servicios

Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todaslas llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos demonitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquierproblema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto ala calidad de la mesa de servicios y de los servicios de TI.

14.1.4 Estructura para la planificación de la continuidad del negocio

Control

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.

Guía de implementación

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan. Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un dueño específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de seguridad de la información identificados y considera los siguientes aspectos:

a) Las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.

b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.

c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.

d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.

e) Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.

f) Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan.

g) Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.

h) Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.

i) Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

Guías de Aseguramiento

- Averiguar y confirmar si una oficina de servicio de TI existe.
- Averiguar y confirmar si el análisis se ha realizado para determinar el modelo de escritorio de servicio, personal, herramientas y la integración con otros procesos.
- Asegúrese de que las horas de operación y tiempo de respuesta se espera a una llamada de cumplir con los requerimientos del negocio.
- Averiguar y confirmar si existen instrucciones para el manejo de una consulta que no pueden ser resueltas de inmediato por el personal de servicio de mesa. Las consultas deberían tener prioridadniveles que determinan el tiempo de resolución deseada y procedimientos de escalamiento.

- Pídale al personal relevante acerca de si las herramientas para el escritorio de servicio se aplican de conformidad con las definiciones y los requisitos de servicio SLA.

- Infórmese sobre la existencia de estándares de servicio y la comunicación de las normas con los clientes.

DS8.2 Registro de Consultas de Clientes

Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades deinformación. Debe trabajar estrechamente con los procesos de administración de incidentes, administración de problemas,administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse deacuerdo al negocio y a la prioridad del servicio y enrutarse al equipo de administración de problemas apropiado y se debe mantenerinformados a los clientes sobre el estatus de sus consultas.

13.1.1 Reporte sobre los eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Guía de implementación

Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empelados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema.

b) formatos para el reporte de los eventos de seguridad de la información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información.

c) el comportamiento correcto en caso de un evento de seguridad de la información, es decir:

    1) tomar nota inmediatamente sobre los detalles importantes (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño).

    2) no ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto.

d) referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de la seguridad.

En entornos de alto riesgo, se puede suministrar una alarma de coacción4) a través de la cual una persona bajo coacción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coacción deberían reflejar la situación de alto riesgo que indican tales alarmas.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

13.2.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Guía de implementación

Además del reporte de los eventos y las debilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades se debería emplear para detectar los incidentes de la seguridad de la información. Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de los incidentes de seguridad de la información:

a) es conveniente instaurar procedimientos para manejar los diferentes tipos de incidentes

de seguridad de la información, incluyendo:

1) fallas en el sistema de información y pérdida del servicio.

2) códigos maliciosos.

3) negación del servicio.

4) errores producidos por datos del negocio incompletos o inexactos.

5) violaciones de la confidencialidad y la integridad.

6) uso inadecuado de los sistemas de información.

b) además de los planes normales de contingencia, los procedimientos también deberían comprender:

1) el análisis y la identificación de la causa del incidente.

2) la contención.

3) la planificación e implementación de la acción correctiva para evitar la recurrencia, si es necesario.

4) la comunicación con aquellos afectados o implicados con la recuperación después del incidente.

5) el reporte de la acción a la autoridad apropiada.

c) se deberían recolectar y asegurar los rastros para auditoría y la evidencia similar, según sea apropiado para:

1) el análisis de los problemas internos;

2) el uso de evidencia forense con respecto a la posible violación del contrato o del requisito reglamentario o en caso de juicios criminales o civiles, por ejemplo, según la legislación sobre uso inadecuado del computador o sobre protección de datos;

3) la negociación para la compensación proveniente de los proveedores de software y servicios;

d) la acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada; los procedimientos deberían garantizar que:

1) únicamente el personal claramente identificado y autorizado tiene acceso a los sistemas y datos activos.

2) todas las acciones de emergencia están documentadas en detalle.

3) la acción de emergencia se reporta a la dirección y se revisa de manera ordenada.

4) la integridad de los sistemas y controles del negocio se confirma con retraso mínimo.

Los objetivos de la gestión de los incidentes de seguridad de la información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de seguridad de la información.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

Guías de Aseguramiento

- Confirme que los procesos y las herramientas están en su lugar para registrar las consultas de los clientes, la situación y las acciones hacia la resolución.
- Evaluar la forma más completa y exacta de este repositorio se mantiene.
- Confirme que el proceso incluye flujo de trabajo para el manejo y la escalada de consultas de los clientes.
- Revisión de una muestra de consultas de los clientes abiertos y cerrados para comprobar el cumplimiento de los compromisos de procesos y servicios.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS8.3 Escalamiento de Incidentes

Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata seanescalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizarque la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de quégrupo de TI esté trabajando en las actividades de resolución.

13.1.2 Reporte sobre las debilidades en la seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

14.1.1 Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguiente elementos clave para la gestión de la continuidad del negocio:

a) Compresión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.

b) Identificación de todos los activos involucrados en los procesos críticos del negocio.

c) Compresión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información y establecer los objetivos de negocio para los servicios de procesamiento de la información.

d) Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.

f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.

g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.

h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio.

i) Prueba y actualización regular de los planes y procesos establecidos.

j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

14.1.4 Estructura para la planificación de la continuidad del negocio

Control

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.

Guía de implementación

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan. Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un dueño específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de seguridad de la información identificados y considera los siguientes aspectos:

a) Las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.

b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.

c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.

d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.

e) Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.

f) Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan.

g) Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.

h) Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.

Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

Guías de Aseguramiento

- Averiguar y confirmar si la oficina de servicio mantiene la propiedad de las solicitudes relacionadas con los clientes y los incidentes.
- Verifique que el ciclo de vida de extremo a extremo de las solicitudes o incidentes se controla adecuadamente y se intensificó por la oficina de servicio.
- Confirmar con los miembros de la gestión de incidentes significativos que se presentan a los mismos.
- Revisar procedimientos de notificación de incidentes significativos para la gestión.
- Confirmar la existencia de un proceso para asegurar que los registros de incidentes se actualizan para mostrar la fecha y hora de la asignación de personal de TI a cada consulta.
- Averiguar y confirmar si hay un proceso en marcha para garantizar que los miembros del personal de TI están involucrados en el tratamiento de las consultas y los incidentes y que el incidentesolicitud de registros se actualizan en todo el ciclo de vida.

DS8.4 Cierre de Incidentes

Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente lamesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

13.2.3 Recolección de evidencias

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

Guía de implementación

Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte.

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastro sólido de la evidencia. En general, dicho rastro sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados.

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

Guías de Aseguramiento

- Averiguar y confirmar si es un proceso para gestionar la resolución de cada incidente.
- Averiguar y confirmar si todos los incidentes resueltos se describen en detalle, incluyendo un registro detallado de todas las medidas para resolver los incidentes.
- Inspeccionar una muestra de los incidentes y compruebe que el estado de la gestión del ciclo de vida del incidente, incluyendo la resolución y el cierre, se informó.

DS8.5 Análisis de Tendencias

Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos derespuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de formacontinua.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

Guías de Aseguramiento

- Averiguar y confirmar si es un proceso para identificar, investigar más a fondo e informar sobre todas las consultas que el acordado plazos para la resolución han ha superado.
- Averiguar y confirmar si, el análisis de tendencias se está realizando en todas las consultas para identificar los incidentes y los patrones de repetición, en apoyo de la identificación del problema.
- Compruebe si la administración de problemas se facilite con regularidad con los datos de análisis de incidentes y tendencias.
- Averiguar y confirmar si, el análisis se realiza sobre la información recibida de los clientes para evaluar los niveles de satisfacción con el servicio prestado por el mostrador de servicio.

- Confirmar la existencia de informes de análisis de comentarios de clientes, y verificar si las acciones correctivas se han adoptado para mejorar el servicio.
- Confirme que el rendimiento del servicio de escritorio se compara con estándares de la industria.
- Compruebe si el análisis de referencia se utiliza para la mejora continua.

Escuchar

Leer fonéticamente

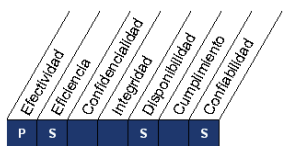
Diccionario - Ver diccionario detallado

DS9 Administrar la Configuración

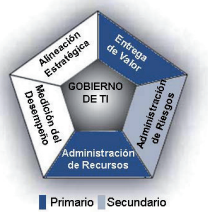
Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio deconfiguraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimientode normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conformese necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción yresuelve los problemas más rápido.

Recurso de TI

Criterios de Información



Gobierno de TI



DS9.1 Repositorio y Línea Base de Configuración

Establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos deconfiguración. Monitorear y grabar todos los activos y los cambios a los activos. Mantener una línea base de los elementos de laconfiguración para todos los sistemas y servicios como punto de comprobación al que volver tras el cambio.

7.2.2 Etiquetado y manejo de la información

Control

Se debería desarrollar e implementar un conjunto de procedimientos adecuados para eletiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado porla organización.

Guía de implementación

Es necesario que los procedimientos para el etiquetado de la información comprendan losactivos de información en formatos físico y electrónico.

Las salidas de los sistemas que contienen información que se clasifica como sensible o críticadeberían portar una etiqueta de clasificación adecuada (en la salida). El etiquetado deberíareflejar la clasificación según las reglas establecidas en el numeral 7.2.1. Los elementos aconsiderar incluyen informes impresos, presentaciones en pantalla, medios grabados (porejemplo, cintas, discos, discos compactos), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación es recomendable definir los procedimientos de manejo,incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucciónseguros.Ello debería incluir los procedimientos para la cadena de custodia y el registro decualquier evento importante de seguridad.

Los acuerdos con otras organizaciones que incluyen compartir información deberían incluirprocedimientos para identificar la clasificación de dicha información y para interpretar lasetiquetas de clasificación de otras organizaciones.

12.4.1 Control del software operativo

Control

Se deberían establecer procedimientos para controlar la instalación de software en los sistemasoperativos.

Guía de implementación

Para minimizar los riesgos de corrupción de los sistemas operativos, se deberían teneren cuenta las siguientes directrices para controlar los cambios:

a) La actualización del software operativo, las aplicaciones y las librerías de los programas sólo deberían ser realizadas por administradores capacitados y con la debida autorización de la dirección.

b) Los sistemas operativos únicamente deberían contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores.

c) El software de las aplicaciones y del sistema operativo sólo se deberían implementar después del ensayo exhaustivo y exitoso; los ensayos deberían incluir pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, igualmente se deberían efectuar en sistemas separados; se debería garantizar que todas las librerías fuente del programa correspondiente estén actualizadas.

d) Se debería usar un sistema de control de configuración para mantener el control el software implementado, así como de la documentación del sistema.

e) Es conveniente instaurar una política de estrategia de restauración al estado anterior antes de implementar los cambios.

f) Se debería conservar un registro para auditoría de todas las actualizaciones de las librerías de los programas operativos.

g) Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.

h) Las versiones antiguas del software se deberían archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

El software suministrado por el vendedor utilizado en los sistemas operativos se deberíamantener en el nivel con soporte del proveedor. Con el tiempo, los vendedores de softwaredejarán de dar soporte a las versiones antiguas del software. La organización deberíaconsiderar los riesgos de depender de software sin soporte.

En toda decisión para mejorar a una nueva versión se debería contar con los requisitos delnegocio para el cambio, y la seguridad de la nueva versión, es decir, la introducción de nuevafuncionalidad en el sistema o la cantidad y gravedad de los problemas de seguridad queafectan a esta versión. Los parches de software se deberían aplicar cuando pueden ayudar aeliminar o reducir las debilidades de la seguridad.

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos desoporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedorse deberían monitorear.

El software de computador puede depender de software y módulos suministradosexternamente, lo cual se debería monitorear y controlar para evitar cambios no autorizados quepuedan introducir debilidades de seguridad.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Guía de implementación

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

Guías de Aseguramiento

- Averiguar y confirmar si la alta dirección establece el alcance y las medidas para las funciones de gestión de la configuración, y evalúa el desempeño.
- Averiguar y confirmar si es una herramienta en su lugar para permitir la aplicación efectiva de registro de información de administración de configuración en un repositorio.
- Determinar que el acceso a la herramienta está restringido al personal apropiado.

- Revisión de una muestra de los elementos de configuración para asegurarse de que un identificador único que se le asigna.
- Averiguar y confirmar si las líneas de base de configuración para los componentes están definidos y documentados.
- Revisar las líneas de base que permita identificar la configuración del sistema en puntos discretos en el tiempo.
- Averiguar y confirmar si hay un proceso documentado para volver a la configuración inicial.
- Prueba de una muestra de los sistemas y las aplicaciones mediante la verificación de que se puede revertir a las configuraciones de referencia.
- Averiguar y confirmar si los mecanismos existen para vigilar los cambios en contra de la línea de base definido y guardamuebles.
- Verifique que la dirección está recibiendo informes regulares y que estos informes de resultado en los planes de mejora continua.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS9.2 Identificación y Mantenimiento de Elementos de Configuración

Establecer procedimientos de configuración para soportar la gestión y rastro de todos los cambios al repositorio de configuración.Integrar estos procedimientos con la gestión de cambios, gestión de incidentes y procedimientos de gestión de problemas.

7.1.1 Inventario de activos

Control

Todos los activos deberían estar claramente identificados y se debería elaborar y mantener uninventario de todos los activos importantes.

Guía de implementación

La organización debería identificar todos los activos y documentar su importancia. El inventariode activos debería incluir toda la información necesaria para recuperarse de los desastres,incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la informaciónsobre licencias y el valor para el negocio. Este inventario no debería duplicar innecesariamenteotros inventarios, pero se debería garantizar que el contenido esté acorde.

Además, se deberían acordar y documentar la propiedad y laclasificación de la información para cada uno de los activos. Con baseen la importancia del activo, su valor para el negocio y su clasificación de seguridad serecomienda identificar los niveles de protección según la importancia de los activos(información adicional sobre la forma de valorar los activos para representar su importancia sepuede encontrar en la norma ISO/IEC TR 13335-3).

7.1.2 Propietario de los activo

Control

Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser propietario de una parte designada de la organización.

Guía de implementación

El propietario del activo debe ser responsable de:

a) Garantizar que la información y los activos asociados con los servicios de procesamiento de la información de clasifican adecuadamente.

b) Definir y revisar periódicamente las restricciones y clasificaciones de los accesos.

La propiedad se puede asignar a:

a) Un proceso de negocio

b) Un conjunto definido de actividades

c) Una aplicación

d) Un conjunto definido de datos

7.2.2 Etiquetado y manejo de la información

Control

Se debería desarrollar e implementar un conjunto de procedimientos adecuados para eletiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado porla organización.

Guía de implementación

Es necesario que los procedimientos para el etiquetado de la información comprendan losactivos de información en formatos físico y electrónico.

Las salidas de los sistemas que contienen información que se clasifica como sensible o críticadeberían portar una etiqueta de clasificación adecuada (en la salida). El etiquetado deberíareflejar la clasificación según las reglas establecidas en el numeral 7.2.1. Los elementos aconsiderar incluyen informes impresos, presentaciones en pantalla, medios grabados (porejemplo, cintas, discos, discos compactos), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación es recomendable definir los procedimientos de manejo,incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucciónseguros.Ello debería incluir los procedimientos para la cadena de custodia y el registro decualquier evento importante de seguridad.

Los acuerdos con otras organizaciones que incluyen compartir información deberían incluirprocedimientos para identificar la clasificación de dicha información y para interpretar lasetiquetas de clasificación de otras organizaciones.

10.7.4 Seguridad de la documentación del sistema

Control

La documentación del sistema debería estar protegida contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) la documentación del sistema se debería almacenar con seguridad.

b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.

c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

11.4.3 Identificación de los equipos en las redes

Control

La identificación automática de los equipos se debería considerar un medio para autenticarconexiones de equipos y ubicaciones específicas.

Guía de implementación

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente sepueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado aéste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estosidentificadores deberían indicar con claridad a qué red está permitido conectar el equipo, siexiste más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesarioconsiderar la protección física del equipo para mantener la seguridad del identificador de éste.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Guía de implementación

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

12.5.3 Restricciones en los cambios a los paquetes de software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.

b) si es necesario obtener el consentimiento del vendedor.

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

Guía de implementación

Un inventario completo y actual de los activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles.

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles.

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche).

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

1) apagar los servicios o capacidades relacionadas con la vulnerabilidad.

2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red.

3) aumentar el monitoreo para detectar o prevenir los ataques reales.

4) crear conciencia sobre la vulnerabilidad.

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados.

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.

j) se deberían tratar primero los sistemas con alto riesgo.

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información

Control

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

Guía de implementación

La dirección debería aprobar el uso de los servicios de procesamiento de información. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio.

Guías de Aseguramiento

- Averiguar y confirmar si la política es para garantizar que todos los elementos de configuración y sus atributos se identifican y se mantiene.
- Averiguar y confirmar si hay una política de etiquetado de activos físicos.
- Verificar que los activos están físicamente etiquetados de acuerdo a la política.
- Averiguar y confirmar si una política de acceso basado en roles existe.
- Verificar que el personal autorizado y adecuado han designado el acceso al depósito de configuración de acuerdo con la política.
- Averiguar y confirmar si la política es para garantizar que el cambio y los procedimientos de gestión de problemas se integran con el mantenimiento del depósito de configuración.

- Averiguar y confirmar si un proceso está en su lugar para grabar nuevos, modificados y eliminados los elementos de configuración, e identificar y mantener las relaciones entre los elementos de configuración en la configuración del repositorio.
- Inspeccione la documentación pertinente, la ejecución oportuna y la integridad de los datos del proceso. Averiguar y confirmar si es un proceso en marcha para asegurar que el análisis se realiza para identificar los elementos de configuración críticos.
- Verifique que apoya este proceso de gestión del cambio y el análisis de las demandas de procesamiento de futuras adquisiciones y la tecnología.
- Averiguar y confirmar si los procedimientos de contratación pública prevén la inscripción de nuevos activos en la herramienta de gestión de la configuración.
- Validar que la gestión de datos coincide con la confirmación de registros de compras.

DS9.3 Revisión de Integridad de la Configuración

Revisar periódicamente los datos de configuración para verificar y confirmar la integridad de la configuración actual e histórica. Revisar periódicamente el software instalado contra la política de uso de software para identificar software personal o no licenciado ocualquier otra instancia de software en exceso del contrato de licenciamiento actual. Reportar, actuar y corregir errores ydesviaciones.

7.1.1 Inventario de activos

Control

Todos los activos deberían estar claramente identificados y se debería elaborar y mantener uninventario de todos los activos importantes.

Guía de implementación

La organización debería identificar todos los activos y documentar su importancia. El inventariode activos debería incluir toda la información necesaria para recuperarse de los desastres,incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la informaciónsobre licencias y el valor para el negocio. Este inventario no debería duplicar innecesariamenteotros inventarios, pero se debería garantizar que el contenido esté acorde.

Además, se deberían acordar y documentar la propiedad y laclasificación de la información para cada uno de los activos. Con baseen la importancia del activo, su valor para el negocio y su clasificación de seguridad serecomienda identificar los niveles de protección según la importancia de los activos(información adicional sobre la forma de valorar los activos para representar su importancia sepuede encontrar en la norma ISO/IEC TR 13335-3).

10.7.4 Seguridad de la documentación del sistema

Control

La documentación del sistema debería estar protegida contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

d) la documentación del sistema se debería almacenar con seguridad.

e) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.

f) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Guía de implementación

Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.

d) garantía de que se hacen cambios en los planes de continuidad del negocio.

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor.

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información

Control

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

Guía de implementación

La dirección debería aprobar el uso de los servicios de procesamiento de información. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio.

Guías de Aseguramiento

- Averiguar y confirmar si es un proceso en marcha para garantizar regularmente la integridad de todos los datos de configuración.
- Revisar los informes que comparan los datos registrados contra el medio ambiente físico.

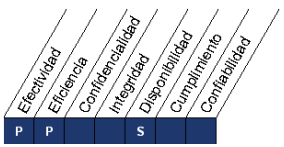
- Verificar que las desviaciones son reportados y corregidos.
- Verifique que el hardware y el software de la reconciliación se realizan periódicamente la base de datos de configuración.
- Si las herramientas automatizadas se utilizan, realizar un manual de la reconciliación con el registro automatizado.
- Verificar que las revisiones periódicas se realizan contra la política de uso de software para la detección de software personal, sin licencia o de cualquier instancia de software por encima de los actuales acuerdos de licencia.

DS10 Administración de Problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde suraíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendacionespara la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo procesode administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.

Recurso de TI

Criterios de Información



Gobierno de TI

DS10.1 Identificación y Clasificación de Problemas

Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes.Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar lacategoría, impacto, urgencia y prioridad. Los problemas deben categorizar se de manera apropiada en grupos o dominiosrelacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidadesorganizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

Guías de Aseguramiento

- Averiguar y confirmar si los procesos adecuados con el apoyo de las herramientas adecuadas para identificar y clasificar los problemas.
- Revisión de los criterios establecidos para clasificar y priorizar los problemas, asegurando que son el resultado en las clasificaciones en línea con los compromisos de servicio y unidades organizativas responsables de resolver o contener el problema.

- Confirme que el proceso está en su lugar por la exactitud de la clasificación, e identificar las razones de los errores de clasificación para que puedan ser tratados.
- Tomar una muestra representativa de la base de datos problema para garantizar que los problemas están debidamente clasificados y categorizados.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS10.2 Rastreo y Resolución de Problemas

El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar ydeterminar la causa raíz de todos los problemas reportados considerando:

• Todos los elementos de configuración asociados

• Problemas e incidentes sobresalientes

• Errores conocidos y sospechados

• Seguimiento de las tendencias de los problemas.

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso deadministración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportesregulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemasdebe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impactose vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado paraincrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. Elavance de la resolución de un problema debe ser monitoreado contra los SLAs.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Guía de implementación

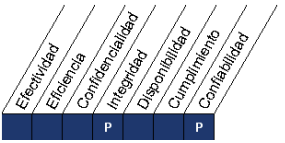
La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

Guías de Aseguramiento

- Confirme que los procesos y las herramientas están en su lugar de registrar, clasificar, priorizar los problemas y realizar un seguimiento de la resolución.
- Confirmar que las herramientas incluyen informes instalaciones que se utilizan para producir informes de gestión sobre los problemas.
- Seleccionar una muestra de informes de problemas y verificar la adecuación de:
  - Problema de la documentación para el análisis de causas raíz.
  - Identificación de los propietarios problema y la responsabilidad de resolución.
  - Problema de la información de estado.

DS11 Administración de Datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración deinformación también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y larecuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad,oportunidad y disponibilidad de la información del negocio.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS11.1 Requerimientos del Negocio para Administración de Datos

Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todoslos resultados se entregan de acuerdo a los requerimientos de negocio. Las necesidades de reinicio y reproceso están soportadas.

10.8.1 Políticas y procedimientos para el intercambio de información

Control

Se deberían establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicio de comunicación.

Guía de implementación

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) Procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.

b) Procedimiento para detección y protección contra código malicioso que se pueden transmitir con el uso de comunicaciones electrónicas.

c) Procedimiento para proteger la información electrónica sensible comunicada que está en forma de adjunto.

d) Políticas o directrices que enfatice el uso aceptable de los servicios de comunicación electrónica.

e) Procedimiento para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.

f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación.

g) Uso de técnicas criptográficas, por ejemplo para proteger la confidencialidad, la integridad y la autenticidad de la información.

h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y reglamentos locales y nacionales correspondientes.

i) No dejar información sensible o critica en los dispositivos de impresión como copiadoras, impresoras y maquinas de facsímil ya que se puede permitir el acceso de personal no autorizado.

j) Controles y restricciones asociados con el envió de servicios de comunicación, como el envió automático de correo electrónico a direcciones de correo externas.

k) Recordar al personal que se deberían tomar precauciones adecuadas como, por ejemplo, no revelar información sensible para evitar que, cuando se hace una llamada telefónica, sea interceptada o escuchada por:

    1. Personas en la cercanía inmediata, particularmente cuando se utiliza teléfonos móviles.

    2. Intercepciones telefónicas o otras formas de escucha no autorizadas mediante el acceso físico al auricular o a la línea telefónica, o usando receptores de exploradores.

    3. Personal al lado del receptor.

l) No dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea.

m) Recordar al personal sobre los problemas de usar maquinas de facsímil a saber:

   1. Creación de acceso no autorizado en los almacenes de mensajes para recuperar los mansajes.

   2. Programación deliberada o accidental de maquinas para enviar mensajes a números específicos.

   3. Envió de documentos y mensajes al número equivocado, bien sea por marcación errónea o por usar el número almacenado erróneamente.

n) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado.

o) Recordar al personal que las maquinas modernas de facsímil y las fotocopiadoras tienen páginas de almacenamiento y caché, en caso de falla en el papel o la transmisión, que se puede imprimir una vez se ha solucionado la falla.

Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

Los servicios de intercambio de información deberían cumplir todos los requisitos legales pertinentes.

Guías de Aseguramiento

- Obtener el inventario de elementos de datos.
- Para cada elemento de datos, confirman que los requisitos de confidencialidad, integridad y disponibilidad se han definido y que estos requisitos han sido validados con los propietarios de los datos.
- Asegúrese de que los controles acordes con los requisitos se han definido e implementado.

DS11.2 Acuerdos de Almacenamiento y Conservación

Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente paraconseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.

10.5.1 Respaldo de la información

Control

Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

Guía de implementación

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información:

a) Es recomendable definir el nivel necesario para la información de respaldo.

b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la organización.

d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.

e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental (véase el numeral 9) consistente con las normas aplicadas en la sede principal; los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo.

f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.

g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación.

h) En situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el periodo de retención de la información esencial para el negocio, así como cualquier requisito para retener permanentemente las copias de archivo.

10.7.1 Gestión de medios removibles

Control

Se debería establecer procedimientos para la gestión de los medios removibles.

Guía de implementación

Se debería tener en cuenta las siguientes directrices:

a) Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se debería hacer irrecuperables.

b) Cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría.

c) Todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.

d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio, también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.

e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente perdida de datos.

f) Las unidades de medios removibles sólo se debería habilitar si existen razones del negocio para hacerlo.

Todos los procedimientos y niveles de automatización deberían estar documentados con claridad.

15.1.3 Protección de los registros de la organización

Control

Los requisitos importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios y contractuales y del negocio.

Guía de implementación

Los registros se deberían clasificar en tipos de registros, por ejemplo registro de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno con los detalles de los periodos de retención y los tipos de medio de almacenamientos como papel, microfichas, medios magnéticos, ópticos, etc. Todo el material relacionado con claves criptográficas y programas asociados a los archivos encriptados o firmas digitales, también se debería almacenar para permitir el descifrado de los registros durante el periodo tiempo durante el cual se retienen los registros.

Es conveniente tomar en consideración la posibilidad de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberían implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso del papel y microfichas.

Al seleccionar los medios de almacenamiento electrónico, se deberían incluir los procedimientos para garantizar la capacidad de acceso a los datos (facilita tanto el medio como el formato) durante todo el periodo de retención para salvaguardar contra pérdida debido a cambio en la tecnología futura.

Los sistemas de almacenamiento de datos de deberían seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.

El sistema de almacenamiento y manipulación debería garantizar la identificación de los registros y su periodo de retención tal como se define en los reglamentos o la legislación nacional o regional, si se aplica. Este sistema debería permitir la destrucción adecuada de los registros después de este periodo, si la organización no los necesita.

Para cumplir estos objetivos de salvaguardia de registros, la organización debería seguir los siguientes aspectos:

a) Se deberían publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registro e información.

b) Es conveniente publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención.

c) Se recomienda conservar un inventario de las fuentes de información clave.

d) Se deberían implementar los controles apropiado para proteger los registros y la información contra pérdida, destrucción y falsificación.

Guías de Aseguramiento

- Revisar el modelo de datos, y asegurar que las técnicas de almacenamiento de satisfacer losrequerimientos del negocio.

- Revisión de los períodos de retención de datos, y asegurar que se ajustan a los requisitos contractuales, legales y reglamentarios.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS11.3 Sistema de Administración de Librerías de Medios

Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidade integridad.

10.7.1 Gestión de medios removibles

Control

Se debería establecer procedimientos para la gestión de los medios removibles.

Guía de implementación

Se debería tener en cuenta las siguientes directrices:

a) Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se debería hacer irrecuperables.

b) Cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría.

c) Todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.

d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio, también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.

e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente perdida de datos.

f) Las unidades de medios removibles sólo se debería habilitar si existen razones del negocio para hacerlo.

Todos los procedimientos y niveles de automatización deberían estar documentados con claridad.

10.7.2 Eliminación de los medios

Control

Cuando ya no se requieren estos medios, su eliminación se debería hacer de forma segura ysin riesgo, utilizando los procedimientos formales.

Guía de implementación

Los procedimientos formales para la eliminación segura de los medios deberían minimizar elriesgo de fuga de información sensible a personas no autorizadas. Los procedimientos para laeliminación segura de los medios que contienen información sensible deberían estar acordescon la sensibilidad de dicha información. Se recomienda tener en cuenta los siguienteselementos.

a) Los medios que contienen información sensible se deberían almacenar y eliminar de forma segura e inocua, por ejemplo mediante incineración o trituración, o borrar los datos para evitar el uso por parte de otra aplicación en la organización.

b) Se deberían establecer procedimientos para identificar los elementos que pueden requerir eliminación segura.

c) Puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma segura, que tratar de disponer sólo de los elementos sensibles.

d) Muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios; se debe tener cuidado en seleccionar un contratista idóneo con controles y experiencia adecuados.

e) Cuando sea posible, se debería registrar la eliminación de los elementos sensibles con el objeto de mantener una prueba de auditoría.

Cuando se acumulan medios para su eliminación se debería considerar el efecto deagregación, el cual puede hacer que una gran cantidad de información no sensible se vuelvasensible.

12.4.3 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implementación

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas, con el objeto de reducir el potencial de corrupción de los programas de computador:

a) cuando sea posible, las librerías fuente de programas no se deberían mantener en los sistemas operativos.

b) el código fuente de programas y las librerías fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.

c) el personal de soporte debería tener acceso restringido a las librerías fuente de programas.

d) la actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.

g) el mantenimiento y el copiado de las librerías fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

Guías de Aseguramiento

- Obtener el inventario de medios de comunicación y, por muestreo, asegúrese de que los medios de comunicación en la lista de inventario pueden ser identificados y elementos de almacenamiento se remonta al inventario.

- A nivel de ejemplo, confirmar que las etiquetas exteriores se corresponden con las etiquetas internas o externas validar que las etiquetas se ponen a los medios de comunicación correcta.

DS11.4 Eliminación

Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y elsoftware se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

9.2.6 Seguridad en la reutilización o eliminación de los equipos

Control

Se deberían verificar todos los elementos del equipo que contengan medios dealmacenamiento para asegurar que se haya eliminado cualquier software licenciado y datossensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.

Guía de implementación

Los dispositivos que contienen información sensible se deberían destruir físicamente o suinformación se debería destruir, borrar o sobrescribir usando técnicas que permitan que lainformación original no se pueda recuperar, en lugar de utilizar las funciones de borrado oformateado estándar.

10.7.1 Gestión de medios removibles

Control

Se debería establecer procedimientos para la gestión de los medios removibles.

Guía de implementación

Se debería tener en cuenta las siguientes directrices:

a) Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se debería hacer irrecuperables.

b) Cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría.

c) Todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.

d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio, también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.

e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente perdida de datos.

f) Las unidades de medios removibles sólo se debería habilitar si existen razones del negocio para hacerlo.

Todos los procedimientos y niveles de automatización deberían estar documentados con claridad.

10.7.2 Eliminación de los medios

Control

Cuando ya no se requieren estos medios, su eliminación se debería hacer de forma segura ysin riesgo, utilizando los procedimientos formales.

Guía de implementación

Los procedimientos formales para la eliminación segura de los medios deberían minimizar elriesgo de fuga de información sensible a personas no autorizadas. Los procedimientos para laeliminación segura de los medios que contienen información sensible deberían estar acordescon la sensibilidad de dicha información. Se recomienda tener en cuenta los siguienteselementos.

a) Los medios que contienen información sensible se deberían almacenar y eliminar de forma segura e inocua, por ejemplo mediante incineración o trituración, o borrar los datos para evitar el uso por parte de otra aplicación en la organización.

b) Se deberían establecer procedimientos para identificar los elementos que pueden requerir eliminación segura.

c) Puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma segura, que tratar de disponer sólo de los elementos sensibles.

d) Muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios; se debe tener cuidado en seleccionar un contratista idóneo con controles y experiencia adecuados.

e) Cuando sea posible, se debería registrar la eliminación de los elementos sensibles con el objeto de mantener una prueba de auditoría.

Cuando se acumulan medios para su eliminación se debería considerar el efecto deagregación, el cual puede hacer que una gran cantidad de información no sensible se vuelvasensible.

Guías de Aseguramiento

Averiguar y confirmar si que:

- La responsabilidad por el desarrollo y la comunicación de las políticas de eliminación está claramente definida.
- Equipos y medios que contienen información sensible son desinfectados antes de su reutilización o eliminación de tal manera que los datos marcados como “eliminados” o “estar dispuesto” no se puede ser recuperados (por ejemplo, los medios de comunicación que contiene datos muy sensibles han sido destruidos físicamente).
- Se dispone el equipo y los medios que contengan información sensible se han registrado para mantener una pista de auditoría.
- Existe un procedimiento para eliminar los medios de comunicación activos de la lista de inventario de los medios de comunicación de su eventual disposición. Compruebe que el inventario actual se ha actualizado para reflejar los últimos cesiones en el registro.
- Equipo de Unsanitised y los medios son transportados de forma segura durante todo el proceso de eliminación.
- Eliminación contratistas tienen la necesaria seguridad física y procedimientos para almacenar y manejar el equipo y los medios de comunicación antes y durante la eliminación.

DS11.5 Respaldo y Restauración

Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea conlos requerimientos de negocio y el plan de continuidad.

10.5.1 Respaldo de la información

Control

Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

Guía de implementación

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información:

a) Es recomendable definir el nivel necesario para la información de respaldo.

b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la organización.

d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.

e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental (véase el numeral 9) consistente con las normas aplicadas en la sede principal; los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo.

f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.

g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación.

h) En situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el periodo de retención de la información esencial para el negocio, así como cualquier requisito para retener permanentemente las copias de archivo.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Los datos críticos que afectan a las operaciones comerciales son periódicamente identificados en la alineación con el modelo de gestión de riesgos y plan de continuidad de servicios de TI.
- Las políticas y procedimientos adecuados para la copia de seguridad de los sistemas, aplicaciones, datos y documentación existentes y considerar factores como:
  - Frecuencia de copia de seguridad (por ejemplo, el reflejo de disco para copias de seguridad en tiempo real frente a DVD-ROM para la retención a largo plazo).
  - Tipo de copia de seguridad (por ejemplo, llena vs incremental).
  - Tipo de medios.
  - Copias de seguridad automatizadas en línea.

- Tipos de datos (por ejemplo, la voz, óptica).
- Creación de registros.
- Crítica de los usuarios finales de datos informáticos (por ejemplo, hojas de cálculo).
- Ubicación física y lógica de las fuentes de datos.
- Seguridad y derechos de acceso.
- Cifrado.

➢ Las responsabilidades se han asignado para la toma de copias de seguridad y vigilancia.

➢ Un programa que existe para la toma y registro de las copias de seguridad de conformidad con laspolíticas y procedimientos establecidos.

➢ El sistema, aplicaciones, datos y documentación mantenido o procesados por terceros sonsuficientemente apoyadas o no asegurado. El regreso de las copias de seguridad de terceroslas partes se deben exigir y consideró los acuerdos de custodia o depósito.

➢ Requisitos para las instalaciones y el almacenamiento fuera del sitio de los datos de copia de seguridad se han definido que cumplan con los requerimientos del negocio, incluyendo el accesonecesario a los datos de copia de seguridad.

➢ Pruebas suficientes de restauración se han realizado periódicamente para asegurar que todos loscomponentes de copias de seguridad pueden ser efectivamente restaurados.

➢ El marco de tiempo requerido para la restauración se ha acordado y se comunicó con el negocio o de TI responsable del proceso. La prioridad para la recuperación de datos se ha basadosobre los requisitos de negocio y procedimientos de continuidad del servicio.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS11.6 Requerimientos de Seguridad para la Administración de Datos

Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo,procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización yrequerimientos regulatorios.

10.5.1 Respaldo de la información

Control

Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

Guía de implementación

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información:

a) Es recomendable definir el nivel necesario para la información de respaldo.

b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la organización.

d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.

e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental (véase el numeral 9) consistente con las normas aplicadas en la sede principal; los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo.

f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.

g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación.

h) En situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el periodo de retención de la información esencial para el negocio, así como cualquier requisito para retener permanentemente las copias de archivo.

10.7.3 Procedimientos para el manejo de la información

Control

Se deberían establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

Guía de implementación

Se deberían elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación. Se deberían considerar los siguientes elementos:

a) manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.

b) restricciones de acceso para evitar el acceso de personal no autorizado.

c) mantenimiento de un registro formal de los receptores autorizados de los datos.

d) garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida.

e) protección, según su nivel de sensibilidad, de los datos de la memoria temporal que esperan su ejecución.

f) almacenamiento de los medios según las especificaciones del fabricante.

g) mantenimiento de la distribución de datos en un mínimo.

h) rotulado claro de todas las copias de los medios para la autenticación del receptor autorizado.

i) revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

10.8.3 Medios físicos en tránsito

Control

Los medios que contienen información se deberían proteger contra el acceso no autorizado, eluso inadecuado o la corrupción durante el transporte más allá de los límites físicos de laorganización.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para la protección de los medios quese transportan entre los lugares:

a) Se recomienda utilizar transporte confiable o servicios de mensajería.

b) Se debería acordar con la dirección una lista de servicios de mensajería.

c) Se deberían desarrollar procedimientos para verificar la identificación de los servicios de mensajería.

d) El embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico potencial que se pueda producir durante el transporte, y estar acorde con las especificaciones del fabricante (por ejemplo para el software), por ejemplo protección contra todos los factores ambientales que puedan reducir la eficacia de la restauración de los medios tal como la exposición al calor, la humedad o los campos electromagnéticos.

e) Cuando sea necesario, se deberían adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada; algunos ejemplos incluyen.

    1) Uso de contenedores cerrados con llave.

    2) Entrega en la mano.

    3) Embalajes con sello de seguridad (que revelan cualquier intento de acceso).

    4) En casos excepcionales, división de la remesa en más de una entrega y despacho por rutas diferentes.

10.8.4 Mensajería electrónica

Control

La información contenida en la mensajería electrónica debería tener la protección adecuada.

Guía de implementación

Las consideraciones de seguridad para la mensajería electrónica deberían incluir lassiguientes:

a) Proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios.

b) Garantizar que la dirección y el transporte del mensaje son correctos.

c) Confiabilidad general y disponibilidad del servicio.

d) Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas.

e) Obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos.

f) Niveles más sólidos de autenticación que controlen el acceso desde redes accesibles al público.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Guía de implementación

Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba.

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

12.4.3 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implementación

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas, con el objeto de reducir el potencial de corrupción de los programas de computador:

a) cuando sea posible, las librerías fuente de programas no se deberían mantener en los sistemas operativos.

b) el código fuente de programas y las librerías fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.

c) el personal de soporte debería tener acceso restringido a las librerías fuente de programas.

d) la actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.

g) el mantenimiento y el copiado de las librerías fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Un proceso está en el lugar que identifica los datos sensibles y las direcciones de las necesidades del negocio de la confidencialidad de los datos, el cumplimiento de las leyes y reglamentos aplicables se ha abordado, y la clasificación de los datos ha sido acordado con los propietarios de procesos de negocio.

- Una política se ha definido e implementado para proteger los datos sensibles y los mensajes del acceso no autorizado y la transmisión incorrecta y el transporte, incluyendo pero no limitado a, el cifrado, los códigos de autenticación de mensajes, totales de control, los correos en régimen de servidumbre y el embalaje a prueba de manipulaciones para el transporte físico.

- Las necesidades se han establecido para el acceso físico y lógico a la salida de datos y la confidencialidad de la producción se define con claridad y tener en cuenta.
- Las normas y procedimientos se han establecido para el acceso de los usuarios finales a los datos de gestión y seguridad de los datos sensibles.
- Las normas y procedimientos se han establecido para las aplicaciones de usuario final que puede ser perjudicial para los datos almacenados en las computadoras de usuario final o las aplicaciones en red o datos (por ejemplo, tenga en cuenta las políticas de derechos de usuario en los ordenadores personales en red).
- Los programas de sensibilización se han instituido para crear y mantener la conciencia de la seguridad en el manejo y tratamiento de datos sensibles.
- Sensible instalaciones de procesamiento de la información están dentro de fronteras seguras ubicaciones físicas protegidas por los perímetros de seguridad definidos junto con la vigilancia adecuada, las barreras de seguridad y controles de entrada.
- El diseño de la infraestructura física previene las pérdidas por el fuego, las interferencias, ataques externos o acceso no autorizado. Hay asegurar los puntos de salida para la recepción de boletas productos sensibles o transferencia de datos a terceros.

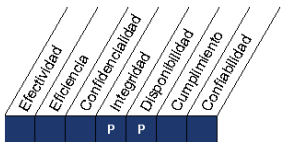
Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS12 Administración del Ambiente Físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso deadministrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección deinstalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. Laadministración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y alpersonal.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS12.1 Selección y Diseño del Centro de Datos

Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategiadel negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastresnaturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones deseguridad y de salud en el trabajo.

9.1.1 Perímetro de seguridad física

Control

Se deberían utilizar perímetros de seguridad (barreras tales como paredes, puertas de accesocontroladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas quecontienen información y servicios de procesamiento de información.

Guía de implementación

Se deberían considerar e implementar las siguientes directrices para los perímetros deseguridad física:

a) Se recomienda definir claramente los perímetros de seguridad y la ubicación y la fortaleza de cada perímetro deberían depender de los requisitos de seguridad de los activos dentro del perímetro, así como de los resultados de la evaluación de riesgos.

b) Los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deberían ser robustos físicamente (es decir, no deberían existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión); las paredes externas del sitio deberían tener una construcción sólida y todas las puertas externas deberían tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debería tener presente la protección externa para las ventanas, particularmente a nivel del suelo.

c) Se debería establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; el acceso a los sitios y edificaciones debería estar restringido únicamente al personal autorizado.

d) Cuando sea viable, se deberían construir barreras físicas para evitar el acceso físico no autorizado y la contaminación ambiental.

e) Todas las puertas de incendio en el perímetro de seguridad deberían tener alarma, monitorearse y someterse a prueba junto con las paredes para establecer el grado requerido de resistencia, según las normas regionales, nacionales e internacionales; éstas deberían funcionar de manera segura de acuerdo con el código local de incendios.

f) Es recomendable la instalación de sistemas adecuados de detección de intrusos según normas nacionales, regionales o internacionales y someterlos a pruebas regularmente para verificar todas las puertas externas y ventanas accesibles; las áreas desocupadas siempre deberían tener alarmas, también se debería tener cubrimiento de otras áreas, por ejemplo los recintos de computadores o de comunicaciones.

g) Los servicios de procesamiento de información dirigidos por la organización deberían estar físicamente separados de aquellos dirigidos por terceras partes.

9.1.3 Seguridad de oficinas, recintos e instalaciones

Control

Se debería diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para la seguridad de oficinas, recintosy servicios:

a) Tener presente los reglamentos y las normas pertinentes a la seguridad y la salud.

b) Las instalaciones claves se deberían ubicar de modo que se evite el acceso al público.

c) Cuando sea viable, las edificaciones deberían ser discretas y no tener indicaciones sobre su propósito, sin señales obvias, fuera o dentro de ellas, que identifiquen la presencia de actividades de procesamiento de información.

d) Los directorios y los listados telefónicos internos que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían ser de fácil acceso al público.

9.1.6 Áreas de carga, despacho y acceso público

Control

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por dondepueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible,aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

Guía de implementación

Se recomienda considerar las siguientes directrices

a) Se debería restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado.

b) El área de despacho y carga se debería designar de forma tal que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

c) Las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas.

d) El material que llega se debería inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.

e) El material que llega se debería registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.

f) Los envíos entrantes y salientes se deberían separar físicamente, cuando sea posible.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Sitios físicos para los equipos informáticos han sido seleccionados de acuerdo a una estrategia de tecnología que cumpla con los requerimientos del negocio y una política de seguridad, teniendo en cuenta cuestiones tales como la posición geográfica, los vecinos, la infraestructura y los riesgos (por ejemplo, el robo, la temperatura, fuego, humo, agua, vibración, el terrorismo, el vandalismo, los productos químicos, explosivos).
- Un proceso se define y aplica que identifica los riesgos potenciales y las amenazas a la organización de TI de los sitios y evalúa el impacto en el negocio de forma continua, teniendo en cuenta el riesgo asociado a los desastres naturales y provocados por el hombre.
- La selección y diseño del sitio, tenga en cuenta las leyes y reglamentos pertinentes, tales como códigos de construcción, el fuego del medio ambiente, ingeniería eléctrica, y salud ocupacional y seguridad.

DS12.2 Medidas de Seguridad Física

Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero nolimitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío yrecepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse lasresponsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

9.1.1 Perímetro de seguridad física

Control

Se deberían utilizar perímetros de seguridad (barreras tales como paredes, puertas de accesocontroladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas quecontienen información y servicios de procesamiento de información.

Guía de implementación

Se deberían considerar e implementar las siguientes directrices para los perímetros deseguridad física:

a) Se recomienda definir claramente los perímetros de seguridad y la ubicación y la fortaleza de cada perímetro deberían depender de los requisitos de seguridad de los activos dentro del perímetro, así como de los resultados de la evaluación de riesgos.

b) Los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deberían ser robustos físicamente (es decir, no deberían existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión); las paredes externas del sitio deberían tener una construcción sólida y todas las puertas externas deberían tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debería tener presente la protección externa para las ventanas, particularmente a nivel del suelo.

c) Se debería establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; el acceso a los sitios y edificaciones debería estar restringido únicamente al personal autorizado.

d) Cuando sea viable, se deberían construir barreras físicas para evitar el acceso físico no autorizado y la contaminación ambiental.

e) Todas las puertas de incendio en el perímetro de seguridad deberían tener alarma, monitorearse y someterse a prueba junto con las paredes para establecer el grado requerido de resistencia, según las normas regionales, nacionales e internacionales; éstas deberían funcionar de manera segura de acuerdo con el código local de incendios.

f) Es recomendable la instalación de sistemas adecuados de detección de intrusos según normas nacionales, regionales o internacionales y someterlos a pruebas regularmente para verificar todas las puertas externas y ventanas accesibles; las áreas desocupadas siempre deberían tener alarmas, también se debería tener cubrimiento de otras áreas, por ejemplo los recintos de computadores o de comunicaciones.

g) Los servicios de procesamiento de información dirigidos por la organización deberían estar físicamente separados de aquellos dirigidos por terceras partes.

9.1.2 Controles de acceso físico

Control

Las áreas seguras deberían estar protegidas con controles de acceso apropiados paraasegurar que sólo se permite el acceso a personal autorizado.

Guía de implementación

Se deberían tener en cuenta las siguientes directrices:

a) Se deberían registrar la fecha y la hora de entrada y salida de visitantes y todos los visitantes deberían estar supervisados, a menos que su acceso haya sido aprobado previamente; sólo se les debería dar acceso para propósitos específicos y autorizados y dicho acceso se debería emitir con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia.

b) Se debería controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas; se deberían utilizar controles de autenticación como las tarjetas de control de acceso más el número de identificación personal (PIN) para autorizar y validar el acceso, se recomienda mantener de forma segura una prueba de auditoría de todos los accesos.

c) Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debería notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante y cualquiera que no use identificación visible.

d) Al personal del servicio de soporte de terceras partes se le debería dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario; éste acceso se debería autorizar y monitorear.

e) Los derechos de acceso a áreas seguras se deberían revisar y actualizar con regularidad y revocados cuando sea necesario.

9.1.3 Seguridad de oficinas, recintos e instalaciones

Control

Se debería diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para la seguridad de oficinas, recintosy servicios:

a) Tener presente los reglamentos y las normas pertinentes a la seguridad y la salud.

b) Las instalaciones claves se deberían ubicar de modo que se evite el acceso al público.

c) Cuando sea viable, las edificaciones deberían ser discretas y no tener indicaciones sobre su propósito, sin señales obvias, fuera o dentro de ellas, que identifiquen la presencia de actividades de procesamiento de información.

d) Los directorios y los listados telefónicos internos que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían ser de fácil acceso al público.

9.2.5 Seguridad de los equipos fuera de las instalaciones

Control

Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Guía de implementación

Independientemente del propietario, la dirección debería autorizar el uso del equipo de procesamiento de información fuera de las instalaciones de la organización.

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo fuera de las instalaciones:

a) El equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes.

b) Se debería observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra explosión a campos electromagnéticos fuertes.

c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgo y controles adecuados que se aplican de forma idónea, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina (ISO/IEC 18028, Seguridad de la red).

d) Se debería establecer el cubrimiento adecuado del seguro para proteger el equipo fuera de las instalaciones.

Los riesgos de seguridad, como daño, robo o escuchas no autorizadas pueden variar considerablemente entre los lugares y se deberían tener en cuenta para determinar los controles más apropiados.

9.2.7 Retiro de activos

Control

Ningún equipo, información ni software se deberían retirar sin autorización previa.

Guía de implementación

Se recomienda tener presentes las siguientes directrices:

a) ni los equipos, ni la información, tampoco el software se deberían retirar sin autorización previa.

b) los empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir retirar activos deberían estar claramente identificados.

c) se recomienda establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de devolución.

d) cuando sea necesario y adecuado, se debería registrar que el equipo ha sido retirado y se debe registrar cuando fue devuelto.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Una política se define y aplica para la seguridad física y las medidas de control de acceso que deben seguirse para TI sitios. La política se revisa periódicamente para asegurarse de que sigue siendo pertinente y actualizada.
- Acceso a la información sobre los sitios sensibles de TI y sus planes de diseño se limita.
- Los signos externos y la identificación de otros sitios sensibles de TI son discretos y no, obviamente, identificar el sitio de fuera.

- Directorios de organización / mapas de sitio no se identifica la ubicación del sitio de TI.
- El diseño de medidas de seguridad física se tiene en cuenta los riesgos asociados con el negocio y la operación. Cuando proceda, medidas de seguridad física incluyen sistemas de alarmas, la creación de endurecimiento, la protección de cables blindados, particiones seguras, etc.
- Pruebas detectivo, preventivo, correctivo y medidas de seguridad física se realizan periódicamente para verificar el diseño, aplicación y eficacia.
- El diseño del sitio tiene en cuenta el cableado físico de las telecomunicaciones y tuberías de agua, electricidad y alcantarillado.
- Un proceso con el apoyo de la autorización correspondiente se define y aplica para la eliminación segura de los equipos informáticos.
- Recepción y envío de las áreas de los equipos informáticos estén protegidos de la misma forma y alcance que los sitios normales de TI y operaciones.
- Una política y el proceso se definen para transportar y almacenar el equipo de forma segura.
- Existe un proceso para asegurar que los dispositivos de almacenamiento que contienen información sensible son físicamente destruidos o desinfectados.
- Existe un proceso para registrar, controlar, gestionar, informar y resolver incidentes de seguridad física, de acuerdo con el proceso de manejo de incidentes de TI global.
- Sitios especialmente sensibles se revisan con frecuencia (incluyendo fines de semana y días festivos) por personal de seguridad.

DS12.3 Acceso Físico

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con lasnecesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse ymonitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores,visitantes o cualquier tercera persona.

6.2.1 Identificación de los riesgos relacionado con las partes externas

Control

Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

Guía de implementación

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgo (**Evaluación y tratamiento del riesgo**) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se debería considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:

1) Acceso físico, por ejemplo a oficinas, recinto de computadores y gabinetes de archivos.

2) Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización.

3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.

4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.

d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.

e) El personal de la parte externa involucrado en manejar la información de la organización.

f) La forma en que se puede identificar a la organización o a al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.

g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.

h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa.

i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta.

k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión y de acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad, que resultan del trabajo con las partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa.

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de la información de la organización.

9.1.2 Controles de acceso físico

Control

Las áreas seguras deberían estar protegidas con controles de acceso apropiados paraasegurar que sólo se permite el acceso a personal autorizado.

Guía de implementación

Se deberían tener en cuenta las siguientes directrices:

a) Se deberían registrar la fecha y la hora de entrada y salida de visitantes y todos los visitantes deberían estar supervisados, a menos que su acceso haya sido aprobado previamente; sólo se les debería dar acceso para propósitos específicos y autorizados y dicho acceso se debería emitir con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia.

b) Se debería controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas; se deberían utilizar controles de autenticación como las tarjetas de control de acceso más el número de identificación personal (PIN) para autorizar y validar el acceso, se recomienda mantener de forma segura una prueba de auditoría de todos los accesos.

c) Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debería notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante y cualquiera que no use identificación visible.

d) Al personal del servicio de soporte de terceras partes se le debería dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario; éste acceso se debería autorizar y monitorear.

e) Los derechos de acceso a áreas seguras se deberían revisar y actualizar con regularidad y revocados cuando sea necesario.

9.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) el personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida.

b) se debería evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.

c) las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente.

d) no se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.

9.1.6 Áreas de carga, despacho y acceso público

Control

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por dondepueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible,aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

Guía de implementación

Se recomienda considerar las siguientes directrices

a) Se debería restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado.

b) El área de despacho y carga se debería designar de forma tal que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

c) Las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas.

d) El material que llega se debería inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.

e) El material que llega se debería registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.

f) Los envíos entrantes y salientes se deberían separar físicamente, cuando sea posible.

9.2.5 Seguridad de los equipos fuera de las instalaciones

Control

Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Guía de implementación

Independientemente del propietario, la dirección debería autorizar el uso del equipo de procesamiento de información fuera de las instalaciones de la organización.

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo fuera de las instalaciones:

a) El equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes.

b) Se debería observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra explosión a campos electromagnéticos fuertes.

c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgo y controles adecuados que se aplican de forma idónea, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina (ISO/IEC 18028, Seguridad de la red).

d) Se debería establecer el cubrimiento adecuado del seguro para proteger el equipo fuera de las instalaciones.

Los riesgos de seguridad, como daño, robo o escuchas no autorizadas pueden variar considerablemente entre los lugares y se deberían tener en cuenta para determinar los controles más apropiados.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Un proceso está en el lugar que regula la solicitud y concesión de acceso a las instalaciones de computación.
- Las solicitudes formales de acceso se han completado y autorizado por la dirección del sitio de TI, los registros se conservan, y las formas específicamente identificar las áreas en que el individuo tiene acceso. Esto se verifica mediante la observación o la revisión de las autorizaciones.
- Se han establecido procedimientos para garantizar que los perfiles de acceso siguen siendo actuales. Compruebe que el acceso a sitios de TI (salas de servidores, edificios, áreas o zonas) se basa en la función de trabajo y responsabilidades.
- Hay un proceso para registrar y monitorear todos los puntos de entrada para los sitios, el registro de todos los visitantes, incluidos los contratistas y proveedores, en el sitio.
- Una política existe instruir a todo el personal para mostrar identificación visible en todo momento y evita la emisión de tarjetas de identidad o insignias sin la debida autorización. Observar si se están usando insignias en la práctica.
- Una política existe visitantes que requieren ser acompañados en todo momento por un miembro de la TI en el lugar, mientras que las operaciones de grupo, y los individuos que no se use el equipoidentificación se señalan al personal de seguridad.
- El acceso a los sitios sensibles de TI está restringido a través de restricciones perímetro, tales como cercas o paredes y los dispositivos de seguridad en las puertas interiores y exteriores. Compruebe que la entrada de dispositivos de registro y sonido de una alarma en caso de acceso no autorizado. Ejemplos de tales dispositivos incluyen placas o tarjetas llave, teclados, circuito cerrado de televisión y escáneres biométricos.

- Regular el entrenamiento físico acerca de la seguridad se lleva a cabo. Verificar mediante la revisión de los registros de capacitación.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS12.4 Protección Contra Factores Ambientales

Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado paramonitorear y controlar el ambiente.

9.1.4 Protección contra amenazas externas y ambientales

Control

Se deberían diseñar y aplicar protecciones físicas contra daño por incendio, inundación,terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Guía de implementación

Se deben tener en cuenta todas las amenazas para la seguridad que presentan lasinstalaciones circundantes, por ejemplo, un incendio en la edificación contigua, fuga de aguapor un techo o en los pisos por debajo del nivel del suelo o una explosión en la calle.

Se recomienda tener en mente las siguientes directrices para evitar daño debido a incendio,inundación, terremoto, explosión, malestar social, y otras formas de desastre natural o artificial:

a) Los materiales combustibles o peligrosos se deberían almacenar a una distancia prudente del área de seguridad. Los suministros a granel tales como los materiales de oficina, no se deberían almacenar en un área segura.

b) Los equipos de repuesto y los medios de soporte de seguridad se deberían ubicar a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales.

c) Se debería suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.

9.2.1 Ubicación y protección de los equipos

Control

Los equipos deberían estar ubicados o protegidos para reducir el riesgo debido a amenazas opeligros del entorno, y las oportunidades de acceso no autorizado.

Guía de implementación

Se recomienda considerar las siguientes directrices para la protección de los equipos:

a) Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo.

b) Los servicios de procesamiento de información que manejan datos sensibles, deberían estar ubicados de forma tal que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento se deberían asegurar para evitar el acceso no autorizado.

c) Los elementos que requieran protección especial deberían estar aislados para reducir el nivel general de protección requerida de los demás elementos.

d) Se recomienda adoptar controles para minimizar el riesgo de amenazas físicas potenciales, por ejemplo robo, incendio, explosión, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia con el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.

e) Se deberían establecer directrices para comer, beber y fumar en las cercanías de los servicios de procesamiento de información.

f) Es conveniente monitorear las condiciones ambientales, como temperatura y humedad, para determinar las condiciones que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información.

g) Se debería aplicar protección contra rayos a todas las edificaciones y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación.

h) Es recomendable considerar la utilización de métodos especiales de protección para equipos en ambientes industriales, tales como membranas para los teclados.

i) Los equipos de procesamiento de información sensible deberían estar protegidos para minimizar el riesgo de fuga de información debido a filtración.

9.2.2 Servicios de suministro

Control

Los equipos deberían estar protegidos contra fallas en el suministro de energía y otrasanomalías causadas por fallas en los servicios de suministro.

Guía de implementación

Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción /ventilación y aire acondicionado deberían ser adecuados para los sistemas a los que danapoyo. Los servicios de suministro se deberían inspeccionar regularmente y someter a laspruebas apropiadas para garantizar su funcionamiento adecuado y reducir cualquier riesgodebido a su mal funcionamiento o falla. Se recomienda proporcionar un suministro eléctricoacorde con las especificaciones del fabricante del equipo.

Se recomienda el suministro de energía sin interrupción (UPS) para dar soporte al cierreordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para elnegocio. Los planes de contingencia deberían incluir la acción que se ha de tomar en caso defalla de la UPS. Se recomienda pensar en una planta de energía alterna, si se requiere lacontinuidad del procesamiento en caso de fallas energéticas prolongadas. Debería estardisponible un suministro adecuado de combustible para garantizar que el generador puedafuncionar por un periodo prolongado. El equipo de UPS y los generadores se deberían revisarcon regularidad para asegurarse de que tienen la capacidad adecuada y someterse a pruebasegún las recomendaciones del fabricante. Además, se debe estudiar el uso de fuentesmúltiples de energía o, si el lugar es grande, una subestación de energía independiente.

Los interruptores de emergencia para apagar la energía deberían estar cerca de las salidas deemergencia en los recintos de los equipos para facilitar el corte rápido de energía en caso deemergencia. Se recomienda tener iluminación de emergencia en caso de falla del suministroprincipal.

El suministro de agua debería ser estable y adecuado para alimentar el aire acondicionado, elequipo de humidificación y los sistemas de extinción de incendios (cuando se utilizan). Elfuncionamiento inadecuado en el sistema de suministro de agua puede dañar el equipo o evitarla acción eficaz de la extinción de incendios. Se debería valorar e instalar, si se requiere, unsistema de alarma para detectar el funcionamiento inadecuado en los servicios de soporte.

El equipo de telecomunicaciones se debería conectar al proveedor del servicio mediante almenos dos rutas diferentes para evitar que la falla en una ruta de conexión elimine los serviciosde voz. Estos servicios deberían ser adecuados para satisfacer los requisitos legales localespara comunicaciones de emergencia.

9.2.3 Seguridad del cableado

Control

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soportea los servicios de información debería estar protegidos contra interceptaciones o daños.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para la seguridad del cableado:

a) Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada.

b) El cableado de la red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas.

c) Los cables de energía deberían estar separados de los cables de comunicaciones para evitar interferencia.

d) Se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones accidentales de cables erróneos a la red.

e) Es recomendable emplear un plano del cableado para reducir la posibilidad de errores.

f) Para sistemas críticos o sensibles considerar controles adicionales incluyendo:

   1) Instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación.

   2) Uso de medios alternos de enrutamiento y / o transmisión que suministren seguridad adecuada.

3) Uso de cableado de fibra óptica.

4) Uso de cubiertas (blindaje) electromagnéticas para proteger los cables.

5) Inicio de reconocimientos técnicos e inspecciones físicas en busca de dispositivos no autorizados conectados al cableado.

6) Acceso controlado a los módulos de cableado (patch panel) y a cuartos de cableado.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Existe un proceso para identificar naturales y desastres provocados por el hombre-que podría ocurrir en la zona en la que las instalaciones de la TI sensibles se encuentran. Examen de los informes que verificar que el impacto potencial es evaluado de acuerdo a los procedimientos de planificación de la continuidad.

- Una política es en el lugar que describen cómo los equipos informáticos, incluidos los equipos móviles y fuera del sitio, está protegido contra el robo y las amenazas del medio ambiente. Revisión documentación para garantizar que la política, por ejemplo, barras de comer, beber o fumar en las zonas sensibles, y prohíbe el almacenamiento de suministros de papelería y otros que presentan un riesgo de incendio dentro de las salas de ordenadores.

- TI instalaciones están situadas y construidas de manera de minimizar y mitigar la susceptibilidad a las amenazas ambientales.

- Los dispositivos más apropiados son en el lugar que detectará las amenazas ambientales. Inspeccione el monitoreo continuo hecho en estos dispositivos.

- Las alarmas o notificaciones otros se plantean en el caso de una exposición ambiental, procedimientos de respuesta a estos hechos están documentados y probados, y el personal recibir una formación adecuada.
- Un proceso está en su lugar de comparar las medidas y planes de contingencia frente a los requisitos de la póliza de seguro. Examen de los informes y la póliza de seguro para verificar el cumplimiento.
- Administración tome medidas para garantizar que todos los puntos de incumplimiento se tratan de manera oportuna.
- TI sitios se construyen en lugares que minimicen el impacto de riesgo ambiental, tales como el robo, aire, fuego, humo, agua, la vibración, el terrorismo y el vandalismo. Físicamente inspeccionar la ubicación de los sitios de TI para garantizar que el diseño se aplica correctamente. Revise el informe de evaluación del riesgo efectuada con anterioridad al diseño y construcción del sitio.
- Una política está en el lugar para garantizar la limpieza permanente y de limpieza en las inmediaciones de las operaciones de TI. Compruebe la TI sitios y salas de servidores para asegurarse que se mantienen en uncondición limpia, ordenada y segura en todo momento (por ejemplo, ningún lío / cajas de arena, papel o cartón, llena de cubos de basura, productos químicoso materiales inflamables). Pregunte si los sitiossiempre se mantienen limpias.

DS12.5 Administración de Instalaciones Físicas

Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y losreglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

9.2.2 Servicios de suministro

Control

Los equipos deberían estar protegidos contra fallas en el suministro de energía y otrasanomalías causadas por fallas en los servicios de suministro.

Guía de implementación

Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción /ventilación y aire acondicionado deberían ser adecuados para los sistemas a los que danapoyo. Los servicios de suministro se deberían inspeccionar regularmente y someter a laspruebas apropiadas para garantizar su funcionamiento adecuado y reducir cualquier riesgodebido a su mal funcionamiento o falla. Se recomienda proporcionar un suministro eléctricoacorde con las especificaciones del fabricante del equipo.

Se recomienda el suministro de energía sin interrupción (UPS) para dar soporte al cierreordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para elnegocio. Los planes de contingencia deberían incluir la acción que se ha de tomar en caso defalla de la UPS. Se recomienda pensar en una planta de energía alterna, si se requiere lacontinuidad del procesamiento en caso de fallas energéticas prolongadas. Debería estardisponible un suministro adecuado de combustible para garantizar que el generador puedafuncionar por un periodo prolongado. El equipo de UPS y los generadores se deberían revisarcon regularidad para asegurarse de que tienen la capacidad adecuada y someterse a pruebasegún las recomendaciones del fabricante. Además, se debe estudiar el uso de fuentesmúltiples de energía o, si el lugar es grande, una subestación de energía independiente.

Los interruptores de emergencia para apagar la energía deberían estar cerca de las salidas deemergencia en los recintos de los equipos para facilitar el corte rápido de energía en caso deemergencia. Se recomienda tener iluminación de emergencia en caso de falla del suministroprincipal.

El suministro de agua debería ser estable y adecuado para alimentar el aire acondicionado, elequipo de humidificación y los sistemas de extinción de incendios (cuando se utilizan). Elfuncionamiento inadecuado en el sistema de suministro de agua puede dañar el equipo o evitarla acción eficaz de la extinción de incendios. Se debería valorar e instalar, si se requiere, unsistema de alarma para detectar el funcionamiento inadecuado en los servicios de soporte.

El equipo de telecomunicaciones se debería conectar al proveedor del servicio mediante almenos dos rutas diferentes para evitar que la falla en una ruta de conexión elimine los serviciosde voz. Estos servicios deberían ser adecuados para satisfacer los requisitos legales localespara comunicaciones de emergencia.

9.2.4 Mantenimiento de los equipos

Control

Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

Guía de implementación

Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos:

a) el mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.

b) sólo personal de mantenimiento autorizado debería realizar las reparaciones y el servicio de los equipos.

c) se recomienda conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo.

d) es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización; cuando sea necesario, la información sensible se debería retirar del entorno del equipo o el personal de mantenimiento debería ser suficientemente revisado.

e) se deberían cumplir todos los requisitos impuestos por las pólizas de seguros.

Guías de Aseguramiento

- Averiguar si y confirmar que:
  - Existe un proceso que examina la necesidad de servicios de TI "para la protección contra las condiciones ambientales y las fluctuaciones de potencia y apagones, en conjunción con otros procedimientos de planificación de la continuidad.
  - Sistemas de alimentación ininterrumpida (SAI) son adquiridos y cumplir con los requisitos de disponibilidad y continuidad del negocio.
  - Un proceso está en su lugar para poner a prueba periódicamente el funcionamiento del UPS y para garantizar que el poder puede cambiar a la red sin ningún efecto significativo en las operaciones de negocio.
  - Las pruebas se han realizado y se tomen medidas correctoras cuando sea necesario.
  - En las instalaciones de la vivienda los sistemas informáticos sensibles, más de una entrada de alimentación está disponible.
  - La entrada física de la energía se separa.

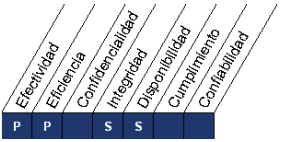
- Sitio de cableado externo a la TI se encuentra bajo tierra o tiene otro tipo de protección adecuada.
- Los planos y los planes existentes.
- Sitio de cableado en el que está contenido dentro de los conductos asegurado.
- El cableado está protegido y endurecido en contra del riesgo medioambiental.
- Armarios de cableado están cerrados con acceso restringido.
- Cableado y física de parches (datos y teléfono) están bien estructurados y organizados.
- Documentación para el cableado y los conductos se encuentra disponible para la referencia.
- Para las viviendas sistemas de alta disponibilidad, el análisis se hace para redundancia y fail-over requisitos de cableado (externa e interna).
- Existe un proceso para garantizar que los sitios de TI y las instalaciones están en el cumplimiento con las leyes pertinentes de salud y seguridad, reglamentos, directrices, o vendedor especificaciones.
- Un proceso está en su lugar para educar al personal sobre las leyes de salud y seguridad, reglamentos o directrices. Esto también incluye la educación del personal en los simulacros de incendio y rescate para garantizar el conocimiento y las acciones realizadas en caso de incendio o de incidentes similares.
- El programa de capacitación evalúa el conocimiento de las directrices y el programa de capacitación se documenta.

- Existe un proceso para registrar, controlar, gestionar y resolver las incidencias en las instalaciones de acuerdo con el proceso de TI de gestión de incidentes.
- Informes sobre incidentes se ponen a disposición cuya divulgación se requiere en términos de las leyes y reglamentos.
- Existe un proceso para garantizar que los sitios de TI y el equipo se mantienen los intervalos del proveedor de servicios y especificaciones recomendadas.
- El mantenimiento es realizado sólo por personal autorizado. Revisar la documentación y consultar a personal para confirmar.
- Las alteraciones físicas de TI o en los locales se analizan para reevaluar el riesgo ambiental (por ejemplo, incendios, daños por agua).
- Los resultados de este análisis se informó a la continuidad del negocio y gestión de instalaciones.

- Camine por las instalaciones y comparar los resultados con las directrices de salud y seguridad.
- Pregunte al personal sobre las posibles violaciones de las normas.
- Camine a través de sitios cambiado recientemente para garantizar que siguen cumpliendo las normas de riesgos.

DS13 Administración de Operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y delmantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administraciónefectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimientopreventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce losretrasos en el trabajo y los costos operativos de TI.

Recurso de TI	Criterios de Información	Gobierno de TI
		

DS13.1 Procedimientos e Instrucciones de Operación

Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones estáfamiliarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos deentrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos deescalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

10.1.1 Documentación de los procedimientos de operación

Control

Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

Guía de implementación

Se deberían elaborar procedimientos documentados para las actividades del sistema asociadas con los servicios de comunicaciones y de procesamiento de información, como por ejemplo procedimientos para el encendido y apagado de los computadores, copias de respaldo, mantenimiento de equipos, manejo de los medios, cuarto de equipos y gestión del correo, como también de la seguridad.

Los procedimientos de operación deberían especificar las instrucciones para la ejecución detallada de cada trabajo, incluyendo:

a) procesamiento y manejo de información.

b) copias de respaldo.

c) requisitos de programación, incluyendo las interrelaciones con otros sistemas, hora de comienzo de la tarea inicial y de terminación de la tarea final.

d) instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.

e) contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

f) Instrucciones de manejo de los medios y los informes especiales, como el uso de papelería especial o el manejo de los informes confidenciales incluyendo los procedimientos para la eliminación segura de los informes de tareas fallidas.

g) procedimientos para el reinicio y la recuperación del sistema que se han de usar en caso de falla del sistema.

h) gestión de los registros de auditoría y de la información de registro del sistema.

Los procedimientos operativos, y los procedimientos documentados para las actividades del sistema, se deberían tratar como documentos formales y sus cambios deberían ser autorizados por la dirección. Cuando sea técnicamente viable, se recomienda gestionar los sistemas de información de forma consistente, utilizando los mismos procedimientos, herramientas y utilidades.

10.7.4 Seguridad de la documentación del sistema

Control

La documentación del sistema debería estar protegida contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) la documentación del sistema se debería almacenar con seguridad.

b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.

c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

Guías de Aseguramiento

- Revise una copia de la norma los procedimientos operativos de TI.

- Revisión de los procedimientos operativos para la integridad. El contenido puede incluir funciones y responsabilidades de los miembros del personal de TI, los organigramas, las funciones de supervisor y directa informes, procedimientos de terminación anormal del sistema operativo, una lista de llamada en caso de emergencia, etc.

- Inspeccione el organigrama y revisar los papeles de trabajo.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

DS13.5 Mantenimiento Preventivo del Hardware

Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y elimpacto de las fallas o de la disminución del desempeño.

9.2.4 Mantenimiento de los equipos

Control

Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

Guía de implementación

Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos:

a) el mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.

b) sólo personal de mantenimiento autorizado debería realizar las reparaciones y el servicio de los equipos.

c) se recomienda conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo.

d) es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización; cuando sea necesario, la información sensible se debería retirar del entorno del equipo o el personal de mantenimiento debería ser suficientemente revisado.

e) se deberían cumplir todos los requisitos impuestos por las pólizas de seguros.

Guías de Aseguramiento

Averiguar si y confirmar que:

- Un plan de mantenimiento preventivo para todo el hardware crítica está en su lugar y que se ha diseñado teniendo en cuenta el análisis de costo-beneficio, las recomendaciones del vendedor, el riesgo de interrupción, personal cualificado y otros factores relevantes.
- Actividad de los registros son revisados para la identificación de las necesidades de mantenimiento preventivo, y el impacto esperado (por ejemplo, las restricciones de rendimiento, SLA) de las actividades de mantenimiento se comunica a los clientes afectados y los usuarios.

APÉNDICE D

GUÍAS PARA EL DOMINIO DE MONITOREAR Y EVALUAR

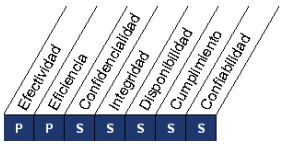
MONITOREAR Y EVALUAR (ME)

ME1 Monitorear y Evaluar el Desempeño de TI

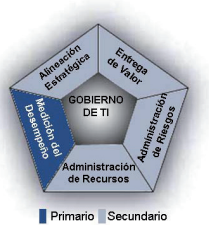
Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores dedesempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. Elmonitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones ypolíticas.

Recurso de TI

Criterios de Información



Gobierno de TI



ME1.2 Definición y Recolección de Datos de Monitoreo

Trabajar con el negocio para definir un conjunto balanceado de objetivos de desempeño y tenerlos aprobados por el negocio y otrosinteresados relevantes. Definir referencias con las que comparar los objetivos, e identificar datos disponibles a recolectar para medirlos objetivos. Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

10.10.2 Monitoreo del uso del sistema

Control

Se deberían establecer procedimientos para el monitoreo del uso de los servicios deprocesamiento de información, y los resultados de las actividades de monitoreo se deberíanrevisar con regularidad.

Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado, incluyendo detalles como:

   1) Identificación de usuario (ID).

   2) Fecha y hora de eventos clave.

   3) Tipo de eventos.

   4) Archivos a los que se ha tenido acceso.

   5) Programas / utilidades empleados.

b) Todas las operaciones privilegiadas como:

   1) Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.

   2) Encendido y detención del sistema.

   3) Acople / desacople del dispositivo de entrada / salida (I/O).

c) Intentos de acceso no autorizado, tales como:

   1) Acciones de usuario fallidas o rechazadas.

2) Acciones fallidas o rechazadas que implican datos y otros recursos.

3) Violaciones de la política de acceso y notificaciones para las barreras de fuego (firewalls) y puertas de enlace (gateways).

4) Alertas de los sistemas de detección de intrusión de propietario.

d) Alertas o fallas del sistema como:

1) Alertas o mensajes de consola.

2) Excepciones de registro del sistema.

3) Alarmas de gestión de red.

4) Alarmas originadas por el sistema de control del acceso.

5) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.

b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.

d) Extensión de la interconexión del sistema (particularmente en redes públicas).

e) Servicio de operación de registro que se desactiva.

Guías de Aseguramiento

Pregunte y confirmar si, que:

- Las metas se han definido para la medición de TI de acuerdo con la cobertura y las características de los indicadores definidos en el marco de seguimiento. Obtener TI y el negocio gestión de la aprobación de los objetivos.
- Los datos de rendimiento que necesita el enfoque de seguimiento se recogen de manera satisfactoria y de forma automatizada, siempre que sea posible. Verifique que el rendimiento se mide en comparación con los objetivos acordados en los intervalos.
- Existen procedimientos para garantizar la coherencia, la integridad y la integridad del control de los rendimientos de origen de datos.
- Existe un proceso para controlar todos los cambios en el rendimiento de datos de vigilancia de fuentes.
- Los objetivos de rendimiento se han definido y se centran en aquellas que proporcionan el mayor ratio de penetración a los esfuerzos.
- La integridad de los datos recogidos se evalúa mediante la realización de la reconciliación y los controles de control en intervalos acordadosEscuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

ME2 Monitorear y Evaluar el Control Interno

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye elmonitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Unbeneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y elcumplimiento de las leyes y regulaciones aplicables.

Recurso de TI	Criterios de Información	Gobierno de TI
		

ME2.1 Monitoreo del Marco de Trabajo de Control Interno

Monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacerlos objetivos organizacionales.

5.1.1 Documento de la política de seguridad de la información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización.

incluyendo los siguientes:

1) cumplimiento de los requisitos legales, reglamentarios y contractuales;

2) requisitos de educación, formación y concientización sobre seguridad;

3) gestión de la continuidad del negocio;

4) consecuencias de las violaciones de la política de seguridad;

e) definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

f) referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

- Evaluar si existe un apoyo a nivel ejecutivo de las normas de gobernanza de la organización para el control interno y gestión de riesgos (por ejemplo, los minutos, las políticascorporativas,entrevista con el consejero delegado). Verificar que las políticas y procedimientos incluyen la gobernanza de las normas internas y la gestión de riesgos (por ejemplo, la adopción de Control Interno COSO- Marco Integrado, Marco COSO Enterprise Risk Management-integrado, COBIT).
- Evaluar si existe un enfoque de mejora continua de seguimiento de control interno (es decir, cuadro de mando integral, la auto-evaluación).

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

ME2.2 Revisiones de Auditoría

Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

10.10.2 Monitoreo del uso del sistema

Control

Se deberían establecer procedimientos para el monitoreo del uso de los servicios deprocesamiento de información, y los resultados de las actividades de monitoreo se deberíanrevisar con regularidad.

Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado, incluyendo detalles como:

   1) Identificación de usuario (ID).

   2) Fecha y hora de eventos clave.

   3) Tipo de eventos.

   4) Archivos a los que se ha tenido acceso.

   5) Programas / utilidades empleados.

b) Todas las operaciones privilegiadas como:

   1) Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.

   2) Encendido y detención del sistema.

   3) Acople / desacople del dispositivo de entrada / salida (I/O).

c) Intentos de acceso no autorizado, tales como:

1) Acciones de usuario fallidas o rechazadas.

2) Acciones fallidas o rechazadas que implican datos y otros recursos.

3) Violaciones de la política de acceso y notificaciones para las barreras de fuego (firewalls) y puertas de enlace (gateways).

4) Alertas de los sistemas de detección de intrusión de propietario.

d) Alertas o fallas del sistema como:

1) Alertas o mensajes de consola.

2) Excepciones de registro del sistema.

3) Alarmas de gestión de red.

4) Alarmas originadas por el sistema de control del acceso.

5) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.

b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.

d) Extensión de la interconexión del sistema (particularmente en redes públicas).

e) Servicio de operación de registro que se desactiva.

10.10.4 Registros del administrador y del operador

Control

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

Guía de implementación

Los registros deberían incluir:

a) La hora en que ocurrió el evento (exitoso o fallido).

b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).

c) Cuál cuenta y cuál administrador u operador estuvo involucrado.

d) Cuáles procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

- Confirme que los controles internos que requieren la supervisión de supervisión y revisión son identificadas, y considerar la criticidad y el riesgo de la TI relacionados con las actividades del proceso (por ejemplo, existencia de clasificación de riesgo de los procesos clave y los controles).

- Asegúrese de que un proceso de escalamiento de problemas identificados por exámenes de control se ha definido.

- Comprender la automatización de seguimiento, control y presentación de informes.

ME2.3 Excepciones de Control

Identificar las excepciones de control, y analizar e identificar sus causas raíz subyacente. Escalar las excepciones de control yreportar a los interesados apropiadamente. Establecer acciones correctivas necesarias.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

- Confirmar que las políticas son los umbrales que se establece para los niveles aceptables de control de excepciones y de control de averías.

- Confirmar que los procedimientos de escalamiento de excepciones de control se han comunicado e informó a las empresas de TI y las partes interesadas (por ejemplo, a través de la intranet, copia impresa procedimientos). Los procedimientos de escalada deben incluir criterios o umbrales para la escalada (por ejemplo, las excepciones de control a menos de una cantidad específica de impacto no es necesario se intensificó, las excepciones de control mayor que una cantidad específica de impacto deben informar inmediatamente a CIO, y las excepciones de control mayor que una cantidad específica de impacto exigirá la notificación inmediata a la junta de directores). Entrevista de gestión para evaluar el conocimiento y el conocimiento de los procedimientos de escalada, así como análisis de causa raíz y presentación de informes.
- Confirme que los individuos se les ha asignado la responsabilidad para el análisis de causa raíz y presentación de informes, así como la resolución de excepción.

ME2.4 Control de Auto Evaluación

Evaluar la completitud y efectividad de los controles de gerencia sobre los procesos, políticas y contratos de TI por medio de unprograma continuo de auto-evaluación.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

- Revisar los procedimientos de control de auto-evaluación para garantizar la inclusión deinformación relevante como el alcance, el enfoque de auto-evaluación, criterios de evaluación, lafrecuencia de la auto-evaluación, los roles y responsabilidades, y los resultados de informes alejecutivo de negocios y de TI interesados (por ejemplo, referencia interna normas de auditoría oprácticas aceptadas en el diseño de auto-evaluación).

- Corroborar con la administración para determinar si las revisiones independientes de auto-evaluación de control se llevan a cabo contra los estándares del sector y las mejores prácticas para garantizarobjetividad y permitir el intercambio de buenas prácticas de control interno (por ejemplo, la evaluación comparativa con los niveles de modelo de madurez a través de organizaciones similares y la industria en cuestión).

ME2.5 Aseguramiento del Control Interno

Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio derevisiones de terceros.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

10.10.2 Monitoreo del uso del sistema

Control

Se deberían establecer procedimientos para el monitoreo del uso de los servicios deprocesamiento de información, y los resultados de las actividades de monitoreo se deberíanrevisar con regularidad.

Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado, incluyendo detalles como:

   1) Identificación de usuario (ID).

   2) Fecha y hora de eventos clave.

   3) Tipo de eventos.

   4) Archivos a los que se ha tenido acceso.

   5) Programas / utilidades empleados.

b) Todas las operaciones privilegiadas como:

   1) Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.

   2) Encendido y detención del sistema.

   3) Acople / desacople del dispositivo de entrada / salida (I/O).

c) Intentos de acceso no autorizado, tales como:

1) Acciones de usuario fallidas o rechazadas.

2) Acciones fallidas o rechazadas que implican datos y otros recursos.

3) Violaciones de la política de acceso y notificaciones para las barreras de fuego (firewalls) y puertas de enlace (gateways).

4) Alertas de los sistemas de detección de intrusión de propietario.

d) Alertas o fallas del sistema como:

1) Alertas o mensajes de consola.

2) Excepciones de registro del sistema.

3) Alarmas de gestión de red.

4) Alarmas originadas por el sistema de control del acceso.

5) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.

b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.

d) Extensión de la interconexión del sistema (particularmente en redes públicas).

e) Servicio de operación de registro que se desactiva.

10.10.4 Registros del administrador y del operador

Control

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

Guía de implementación

Los registros deberían incluir:

a) La hora en que ocurrió el evento (exitoso o fallido).

b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).

c) Cuál cuenta y cuál administrador u operador estuvo involucrado.

d) Cuáles procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

15.2.2 Verificación del cumplimiento técnico

Control

Los sistemas de información se deberían verificar periódicamente para determinar elcumplimiento con las normas de implementación de la seguridad.

Guía de implementación

La verificación del cumplimiento técnico se debería realizar bien sea manualmente (con soportede las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas conexperiencia y / o con la ayuda de herramientas automáticas que generan un informe técnicopara la interpretación posterior por parte del especialista técnico.

Si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tenercuidado puesto que dichas actividades pueden poner en peligro la seguridad del sistema. Talespruebas se deberían planificar, documentar y ser repetibles.

La verificación del cumplimiento técnico únicamente la deberían realizar personas autorizadas ycompetentes o bajo supervisión de dichas personas.

15.3.1 Controles de auditoría de los sistemas de información

Control

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

Guía de implementación

Se deberían tener presente las siguientes directrices:

a) los requisitos de auditoría se deberían acordar con la dirección correspondiente.

b) se debería acordar y controlar el alcance de las verificaciones.

c) las verificaciones se deberían limitar al acceso de sólo lectura del software y los datos.

d) el acceso diferente al de sólo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.

e) los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles.

f) se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.

g) todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar para datos o sistemas críticos.

h) se recomienda documentar todos los procedimientos, requisitos y responsabilidades.

i) la persona que realiza la auditoría debería ser independiente de las actividades auditadas.

Guías de Aseguramiento

- Verificar que las revisiones independientes de control, certificaciones o acreditaciones se realizan periódicamente de acuerdo a los objetivos de riesgo y de negocios, junto con habilidades necesarios externos (por ejemplo, realizar una evaluación anual de riesgos y definir las zonas de riesgo para su revisión).
- Verifique que los resultados de la revisión se ha informado a un nivel de gestión apropiadas (por ejemplo, el comité de auditoría) y las medidas correctoras se ha iniciado.

ME2.6 Control Interno para Terceros

Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de serviciosexternos cumplen con los requerimientos legales y regulatorios y obligaciones contractuales.

6.2.3 Abordaje de la seguridad en los acuerdos con terceras partes

Control

Los acuerdo con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicio a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) Políticas de seguridad de la información.

b) Los controles para asegurar la protección del activo, incluyendo:

   1) Procedimiento para proteger los activos de la organización, incluyendo información, software y hardware.

   2) Todos y los controles y mecanismos de protección física requeridos.

   3) Controles para asegurar la protección contra software malicioso.

   4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.

   5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

   6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.

   7) Restricciones a la copia y a la divulgación de la información y uso de acuerdos de niveles de confidencialidad.

c) La información del usuario y del administrador en métodos, procedimientos y seguridad.

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.

e) Las disposiciones para la transferencia de personal, cuando es apropiado.

f) Las responsabilidades relacionadas con la instalación y el mantenimiento de software y el hardware.

g) La estructura clara y los formatos acordados para la presentación de los informes.

h) El proceso claro y específico para la gestión de cambio.

i) La política de control de acceso, incluyendo:

   1) Diversas razones, requisitos y beneficios de la necesidad de acceso por terceras partes.

   2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

   3) Proceso de autorización para los privilegios y el acceso de usuario.

   4) Requisitos para mantener una lista de las personas autorizadas a usar los servicios que se le ponen a disposición, y de sus derechos y privilegios como relación a tal uso.

   5) Declaración de que el acceso que no se autorice explícitamente está prohibido.

   6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

j) Las disposiciones para el reporte, la notificación y la investigación de los incidentes de la seguridad de la información y las violaciones de la seguridad, así como los incumplimiento de los requisitos establecidos en el acuerdo.

k) La descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad.

l) La meta del nivel de servicio y los niveles inaceptables de servicio.

m) La definición de criterios verificables desempeño, su monitoreo y reporte.

n) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.

o) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.

p) El establecimiento de un proceso de escalada para la solución de problemas.

q) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdos con las prioridades de negocio de la organización.

r) Las responsabilidades civiles correspondientes de las partes del acuerdo.

s) Las responsabilidades relacionada con los asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre la protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si acuerdo implica cooperación con organizaciones en otros países.

t) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copias y la protección de cualquier trabajo en colaboración.

u) La participación de las terceras partes con los subcontratistas y los controle de seguridad que estos subcontratistas necesitan implementar.

v) Las condiciones para la renegociación / terminación del acuerdo.

1) Se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

2) Renegociación de acuerdos si cambian los requisitos de seguridad de la organización.

3) Documentación vigente de la listas de activos, licencias, acuerdos o derechos relacionados con ellos.

10.2.2 Monitoreo y revisión de los servicios por terceros

Control

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares.

Guía de implementación

El monitoreo y la revisión de los servicios por terceros deberían garantizar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos y que los incidentes y problemas de la seguridad de la información se manejan adecuadamente. Ello debería implicar una relación y un proceso de gestión del servicio entre la organización y el tercero para:

a) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos.

b) Revisar los reportes del servicio elaborados por el tercero y acordar reuniones periódicas sobre el progreso, según lo exijan los acuerdos.

c) Suministrar información sobre los incidentes de seguridad de la información, y revisión de esta información por parte de la organización y el tercero, según lo exijan los acuerdos, directrices y los procedimientos de soporte.

d) Revisión de los registros y pruebas de auditoría del tercero con respecto a eventos de seguridad, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado.

e) Resolver y manejar todos los problemas identificados.

La responsabilidad por la gestión de la relación con el tercero se le debería asignar a una persona o a un equipo de gestión del servicio. Además, la organización debería garantizar que el tercero asigna responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos. Se recomienda poner a disposición suficientes habilidades técnicas y recursos para monitorear el cumplimiento de los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Cuando se observan deficiencias en la prestación del servicio se deberían tomar las acciones adecuadas.

La organización debería mantener suficiente control global y no perder de vista todos los aspectos de seguridad para la información sensible o crítica, o de los servicios de procesamiento de información que haya procesado, gestionado o tenido acceso el tercero. La organización debería asegurarse de que conserva visibilidad en las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades e informe / respuesta de los incidentes de seguridad de la información a través de un proceso, estructuras y formatos definidos claramente para la presentación de informes.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

- Confirmar que los requisitos de control interno se tratan en las políticas y procedimientos para los contratos y acuerdos con terceros y que las disposiciones adecuadas para los derechos a la auditoría se incluyen.
- Asegúrese de que hay un proceso en marcha para asegurar que las revisiones se realizan periódicamente para acceder a los controles internos de todas las terceras partes y que cuestiones de incumplimiento se comunican.
- Confirmar que las políticas y procedimientos adecuados para confirmar la recepción de cualquier afirmaciones de control requeridas legales o reglamentarias internas de servicio afectado de terceros proveedores.
- Confirmar que las políticas y procedimientos adecuados para investigar las excepciones, y obtener garantías de que las medidas correctoras apropiadas se han aplicado.

ME2.7 Acciones Correctivas

Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Guía de implementación

Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuada, las normas y cualquier otro requisito de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) Determinar la causa del incumplimiento.

b) Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.

c) Determinar e implementar la acción correctiva apropiada.

d) Revisar la acción correctiva que se ejecuto.

Se debería registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

Guías de Aseguramiento

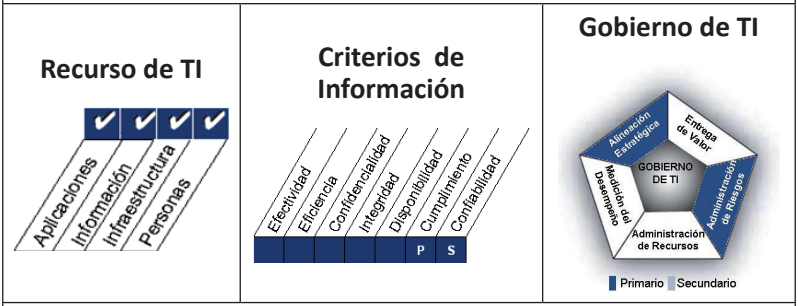
- Confirme que se establezcan procedimientos para iniciar, priorizar y asignar la responsabilidad de todas las acciones correctivas, con el seguimiento adecuado de las acciones.

- Asegúrese de que existe un mecanismo para detectar el comportamiento deficiente de la remediación y que las acciones correctivas son identificadas y revisadas por la administración(Por ejemplo, los hitos del proyecto). Confirme que siguió el desempeño deficiente de la remediación se eleva a la alta dirección para la acción futura (por ejemplo, el estado del proyectopresentación de informes, minutas del comité de dirección de TI).

- Confirmar que los procedimientos establecidos requieren tareas correctivas de acción para ser aprobado después de terminar satisfactoriamente frente a los resultados pre-especificados.

ME3 Garantizar el Cumplimiento con Requerimientos Externos

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento delas leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento,optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrandolos reportes de cumplimiento de TI con el resto del negocio.



ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales

Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben decumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización.

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

15.1.1 Identificación de la legislación aplicable

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

Guía de implementación

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implementación

Se deberían tomar en consideración las siguientes directrices para proteger todo el material que se pueda considerar propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.

b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

c) Mantener la concientización de sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que lo viole.

d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

f) Implementar controles para asegurar que no se excede al número máximo de usuarios permitidos.

g) Verificar que únicamente se instalan software autorizado y productos con licencias.

h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar las herramientas de auditoría adecuada.

k) Cumplir los términos y condiciones para el software y la información obtenido de redes públicas.

l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.

m) No copiar total ni parcialmente libros, archivos, informe ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

Guías de Aseguramiento

- Confirme que se establezcan procedimientos para garantizar que las obligaciones legales, reglamentarias y contractuales que afectan TI son revisados. Estos procedimientos de cumplimiento de la normativa que:
  - ➢ Identificar y evaluar el impacto de los requisitos legales o reglamentarias relacionadas con la organización de TI.
  - ➢ Actualización de las políticas y procedimientos de TI asociados afectados por los requisitos legales y reglamentarios.
  - ➢ Incluir áreas tales como las leyes y reglamentos para el comercio electrónico, el flujo de datos, la privacidad, los controles internos, informes financieros, las regulaciones específicas de la industria, intelectual los derechos de autor de propiedad, y de la salud y la seguridad.
  - ➢ Incluir la frecuencia de revisión de los requisitos legales o reglamentarios (por ejemplo, anualmente o cuando hay un requisito nuevo o actualizado legales, reglamentarias y contractuales).
- Confirme que el registro de todos los requisitos legales, reglamentarios y contractuales, su impacto y acciones requeridas se mantengan y hasta la fecha.

Escuchar

Leer fonéticamente

Diccionario - Ver diccionario detallado

ME3.3 Evaluación del Cumplimiento con Requerimientos Externos

Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios.

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

15.1.1 Identificación de la legislación aplicable

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

Guía de implementación

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implementación

Se deberían tomar en consideración las siguientes directrices para proteger todo el material que se pueda considerar propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.

b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

c) Mantener la concientización de sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que lo viole.

d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

f) Implementar controles para asegurar que no se excede al número máximo de usuarios permitidos.

g) Verificar que únicamente se instalan software autorizado y productos con licencias.

h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar las herramientas de auditoría adecuada.

k) Cumplir los términos y condiciones para el software y la información obtenido de redes públicas.

l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.

m) No copiar total ni parcialmente libros, archivos, informe ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

Guías de Aseguramiento

- Revisar las políticas de TI organización, normas y procedimientos y confirmar su actualización periódica y oportuna para hacer frente a cualquier incumplimiento (legales y reglamentarias)carencias detectadas.

ME3.4 Aseguramiento Positivo del Cumplimiento

Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas orequerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva pararesolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna.

6.1.6 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

15.1.1 Identificación de la legislación aplicable

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

Guía de implementación

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implementación

Se deberían tomar en consideración las siguientes directrices para proteger todo el material que se pueda considerar propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.

b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

c) Mantener la concientización de sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que lo viole.

d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.

f) Implementar controles para asegurar que no se excede al número máximo de usuarios permitidos.

g) Verificar que únicamente se instalan software autorizado y productos con licencias.

h) Suministrar una política para mantener las condiciones de licencia apropiadas.

i) Suministrar una política para la disposición o transferencia de software a otros.

j) Usar las herramientas de auditoría adecuada.

k) Cumplir los términos y condiciones para el software y la información obtenido de redes públicas.

l) No duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.

m) No copiar total ni parcialmente libros, archivos, informe ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

Guías de implementación

Se debería desarrollar e implementar una política de protección y privacidad de los datos, Esta política se debería comunicar a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de los datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrado a una persona responsable, como por ejemplo un funcionario para la protección de datos, quien debería brindar guía a directores, usuario y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concientización sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondiente. Se deberían implementar medidas técnicas y organizacionales apropiadas.

Guías de Aseguramiento

- Revisión del proceso de pruebas de los propietarios de la confirmación periódica del cumplimiento de las leyes, reglamentos y compromisos contractuales (informe, es decir, finales y la letrade los reguladores de reconocer la realización de su examen).

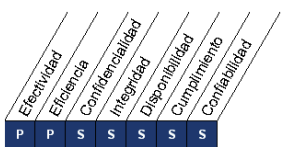
- Revisar que los procesos están en marcha para realizar un seguimiento y ejecución de las revisiones internas y externas para asegurar que no hay una adecuada planificación y asignación de recursos para ayudar o completar las valoraciones (por ejemplo, el inventario de los requisitos reglamentarios, la programación de las revisiones de cumplimiento interno, la programación de los recursos necesarios para ayudar a valoraciones).
- Averiguar si existen procedimientos para evaluar periódicamente los niveles de cumplimiento de los requisitos legales y reglamentarios por partes independientes.
- Revisar las políticas y procedimientos para garantizar que los contratos con proveedores de servicios de terceros requieren confirmación periódica del cumplimiento (por ejemplo, larecepción de declaraciones) conleyes, reglamentos y compromisos contractuales.
- Asegúrese de que un proceso para supervisar e informar sobre incidentes de incumplimiento se aplica, que incluye, donde la investigación es necesario, además de la causa raíz deincidentes que tienen lugar.

ME4 Proporcionar Gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles yresponsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con lasestrategias y objetivos empresariales.

Recurso de TI

Criterios de Información



Gobierno de TI

ME4.7 Aseguramiento Independiente

Garantizar de forma independiente (interna o externa) la conformidad de TI con la legislación y regulación relevante; las políticas de laorganización, estándares y procedimientos; practicas generalmente aceptadas; y la efectividad y eficiencia del desempeño de TI.

5.1.2 Revisión de la política de seguridad de la información

Control:

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación:

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección debería incluir información sobre:

a) Retroalimentación entre las partes interesadas.

b) Resultados de las revisiones independientes.

c) Estados de las acciones preventivas y correctivas.

d) Resultados de las revisiones previas por parte de la dirección.

e) Desempeño del proceso y cumplimento de la política de seguridad de la información.

f) Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de los recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico.

g) Tendencias relacionadas con las amenazas y las vulnerabilidades.

h) Incidentes de seguridad de la información reportados.

i) Recomendaciones de las autoridades pertinentes.

Los resultados de la revisión por la dirección debería incluir todas las decisiones y acciones relacionadas con:

a) Mejorar el enfoque de la organización para la gestión de la seguridad de la información y sus procesos.

b) Mejora de los objetivos de control y de los controles.

c) Mejora de la asignación de recursos y/o responsabilidades.

Es recomendable mantener un registro de la revisión por parte de la dirección.

Se debería obtener la aprobación de la dirección para la política revisada.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

10.10.2 Monitoreo del uso del sistema

Control

Se deberían establecer procedimientos para el monitoreo del uso de los servicios deprocesamiento de información, y los resultados de las actividades de monitoreo se deberíanrevisar con regularidad.

Guía de implementación

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado, incluyendo detalles como:

   1) Identificación de usuario (ID).

   2) Fecha y hora de eventos clave.

   3) Tipo de eventos.

   4) Archivos a los que se ha tenido acceso.

   5) Programas / utilidades empleados.

b) Todas las operaciones privilegiadas como:

   1) Uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador.

   2) Encendido y detención del sistema.

   3) Acople / desacople del dispositivo de entrada / salida (I/O).

c) Intentos de acceso no autorizado, tales como:

1) Acciones de usuario fallidas o rechazadas.

2) Acciones fallidas o rechazadas que implican datos y otros recursos.

3) Violaciones de la política de acceso y notificaciones para las barreras de fuego (firewalls) y puertas de enlace (gateways).

4) Alertas de los sistemas de detección de intrusión de propietario.

d) Alertas o fallas del sistema como:

1) Alertas o mensajes de consola.

2) Excepciones de registro del sistema.

3) Alarmas de gestión de red.

4) Alarmas originadas por el sistema de control del acceso.

5) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.

b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.

d) Extensión de la interconexión del sistema (particularmente en redes públicas).

e) Servicio de operación de registro que se desactiva.

Guías de Aseguramiento

- Averiguar y confirmar si un comité de auditoría ha sido establecido con el mandato de examinar lo que los riesgos son significativos, y evaluar la forma en que se identifican, evaluados y gestionados; comisión de TI y auditorías de seguridad, y con rigor el seguimiento de cierre de las recomendaciones posteriores.

- Entrevista al comité de auditoría y evaluar su conocimiento y conciencia de sus responsabilidades. Determinar si el comité de auditoría establecido está funcionando eficazmente.

- Averiguar y confirmar si los exámenes independientes, certificaciones o acreditaciones de cumplimiento de las políticas, normas y procedimientos se han obtenido. Inspeccionar físicamente para la adecuación de los documentos aportados por las revisiones independientes.